TASK ORDER
47QFCA18F0018

St. Elizabeths Technology Services (SETS)

in support of:

U.S. Department of Homeland Security (DHS)

Issued to:
General Dynamics One Source, LLC

Awarded under GSA Alliant Government-wide
Acquisition Contract GS00Q09BGD0030

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

December 20, 2017

FEDSIM Project Number HS00813

C.1 BACKGROUND

The United States (U.S.) Department of Homeland Security (DHS) is consolidating office space for DHS Headquarters and Component Agencies that are predominately located within the geographical region of the Washington, D.C. metropolitan area (i.e., National Capital Region (NCR)) to the historic St. Elizabeths Campus located in southeast Washington, D.C. It is DHS' intent to move approximately 17,000 employees occupying 12,800 seats onto the St. Elizabeths Campus by Fiscal Year (FY) 2022.

The "DHS Consolidation at St. Elizabeths Draft Enhanced Plan Study Report," dated January 29, 2016, hereafter referenced as the "Enhanced Plan" (Section J, Attachment Tech-A), details the allocation of employees and seats per St. Elizabeths Campus building. Page 37 of the Enhanced Plan is provided as a Microsoft Excel spreadsheet (Section J, Attachment Tech-A1).

In FY 2013, the U.S. Coast Guard (USCG) was the first DHS Component Agency to relocate to the St. Elizabeths Campus and occupy the USCG Headquarters (HQ) Munro Building (i.e., Building 50). On occupancy, the Munro Building IT infrastructure transitioned to Operations and Maintenance (O&M).

The Enhanced Plan includes a notional schedule for construction and rehabilitation. As the facilities become occupied by DHS Component Agencies, the expanded IT infrastructure will transition to O&M.

GSA's Public Buildings Service (PBS) has been and will continue to be responsible for the construction and rehabilitation of St. Elizabeths Campus facilities.

C.1.1 PURPOSE

The purpose of this TO is to provide services to design, procure, configure, implement, test, secure, accredit, operate, and maintain an IT infrastructure for the St. Elizabeths Campus.

C.1.2 AGENCY MISSION

DHS was formed after the terrorist attacks of September 11, 2001, as part of a national effort to safeguard the U.S. against terrorism. Missions include preventing terrorism and enhancing security; securing and managing U.S. borders; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring disaster resilience. The TO will support the DHS mission by providing and ensuring Confidentiality, Integrity, and Availability (CIA) of the St. Elizabeths Campus IT infrastructure on the St. Elizabeths Campus.

C.2 SCOPE

The scope of the TO is to provide IT services for the continued development, expansion, and O&M of the St. Elizabeths Campus IT infrastructure.

The scope of the TO include the following IT services:

a. TO Program Management: This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the Government requirements.

b. Requirements Analysis and Design: This includes identifying technical and functional requirements for the IT infrastructure and the development of engineering designs in conformance with Government technical architectures.

c. Implement and Test: This includes the implementation, operational testing, configuring, accrediting, and transitioning to O&M of all IT infrastructure approved by the Government.

d. O&M: This includes the O&M of the St. Elizabeths Campus IT infrastructure to include the IT Service Desk, Operations Control, Operations Management, IT Security Management, and Technical Management.

e. IT Infrastructure Transitional Services: This includes providing DHS Component Agencies with IT infrastructure transitional services for the evaluation, preparation, and integration of DHS Component Agency's IT infrastructures into the St. Elizabeths Campus IT infrastructure. IT infrastructure transitional services also include the temporary extension of St. Elizabeths Campus IT infrastructure to DHS Component Agency's legacy facilities.

f. TO Transition: This includes both TO transition-in and transition-out activities.

C.3 CURRENT INFORMATION TECHNOLOGY / ENVIRONMENT

The St. Elizabeths Campus IT infrastructure (e.g., fiber active cables, active and passive equipment, application licenses, and data) are owned and managed by the DHS Office of the Chief Information Officer (OCIO).

The St. Elizabeths Campus IT infrastructure supports multiple classification levels, networks, and services. The St. Elizabeths Campus IT infrastructure consists of three physically separate (e.g., isolated) infrastructures delineated by classification levels:

a. SENSITIVE BUT UNCLASSIFIED Campus Area Network (SBUCAN).

b. SECRET Campus Area Network (SCAN).

c. TOP SECRET Campus Area Network (TSCAN).

Each IT infrastructure supports multiple networks and services allocated to the IT infrastructures (i.e., SBUCAN, SCAN, and TSCAN) based on classification. The individual IT infrastructures are also logically partitioned using Virtual Local Area Network (VLAN) technologies.

The St. Elizabeths Campus IT infrastructure currently supports eight networks and services that are subject to Federal Information Security Management Act (FISMA) requirements. The FISMA Identities (IDs) and associated physical IT infrastructures are:

FISMA ID	PHYSICAL INFRASTRUCTURE
St. Es SBUCAN-Production (SBUCAN-P)	SBUCAN
St. Es SBUCAN-Management (SBUCAN-M)	SBUCAN
St. Es Physical Security Network (PSN)	SBUCAN
St. Es Voice Over IP (VoIP)	SBUCAN
St. Es SCAN-Production (SCAN-P)	SCAN
St. Es SCAN-Management (SCAN-M)	SCAN
St. Es TSCAN-Production (TSCAN-P)	TSCAN

FISMA ID	PHYSICAL INFRASTRUCTURE
St. Es TSCAN-Management (TSCAN-M)	TSCAN

The “St. Elizabeths Campus Operations and Maintenance Information Technology Service Provider Concept of Operations” document herein referenced as the “CONOPS” (Section J, Attachment Tech-B) details the networks and services transported on the St. Elizabeths Campus IT infrastructure.

The St. Elizabeths Campus IT physical architecture (Section J, Attachment Tech-U) is comprised of Commercial Off-the-Shelf (COTS) systems using Reconfigurable Optical Add-Drop Multiplexers (ROADMs), Gigabit Passive Optical Networks (GPON), and Ethernet technologies as the transport mechanisms. The St. Elizabeths Campus IT Infrastructure Equipment List is provided as a TOR Attachment (Section J, Attachment Tech-V).

Figures 1.1 and 1.2 provide various diagrams of the St. Elizabeths Campus Physical Architecture; expanded views of Figure 1.1 are included in Figures 1.3, 1.4, and 1.5.

The labels “SECRET” and “TS/SCI” (Top Secret/Sensitive Compartmented Information) in Figures 1.1 and 1.5 identify the SCAN and TSCAN physical IT infrastructures and are not document classification markings.

Figure 1.1 St. Elizabeths Campus Physical Architecture

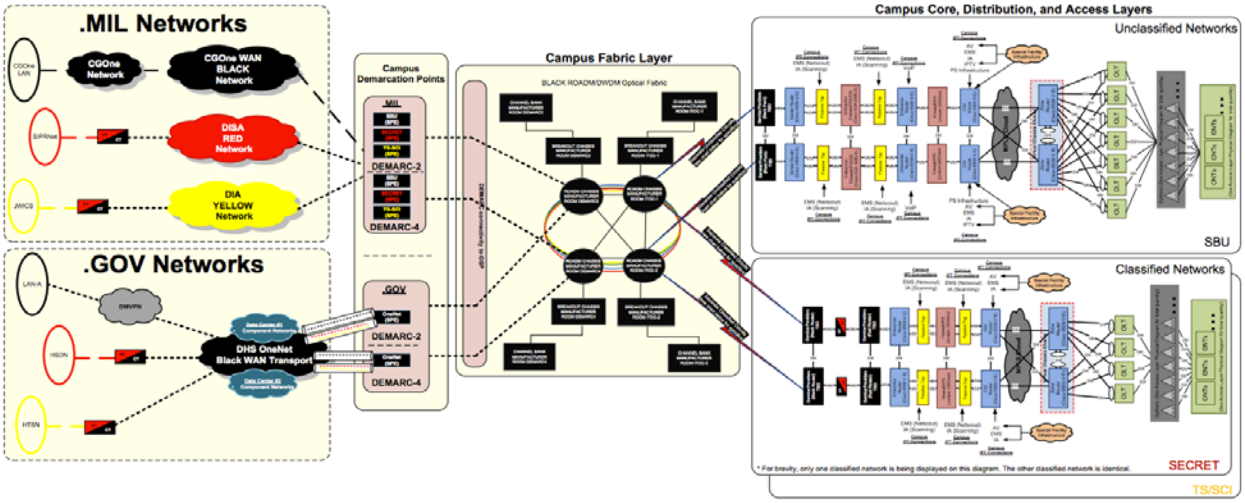
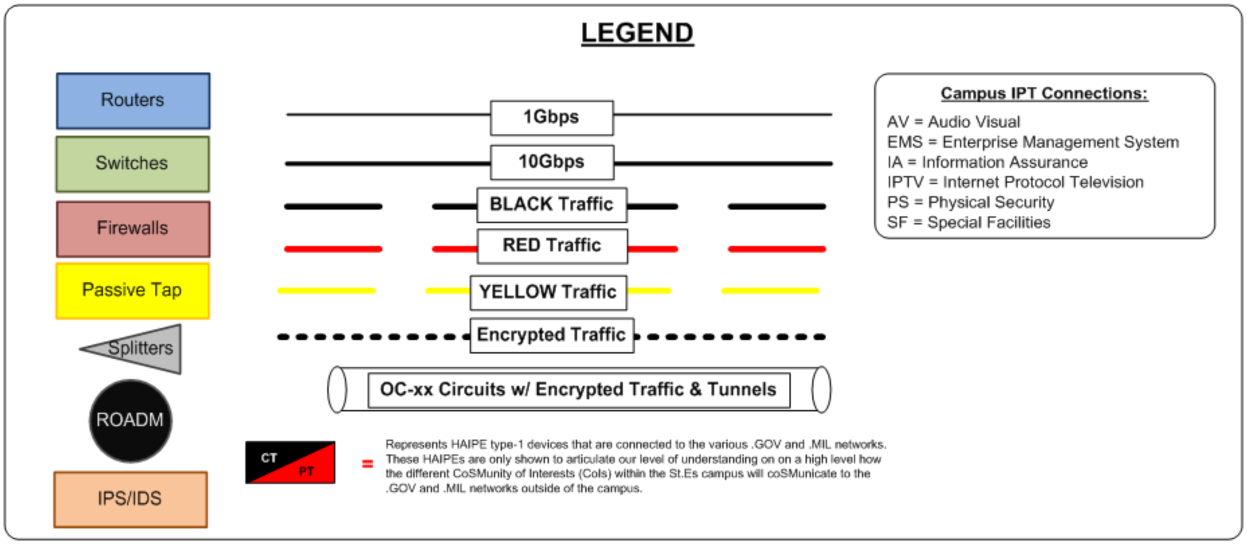

.MIL Networks
CGOne LAN
CGOne Network
CGOne WAN BLACK Network
SIPRNet
DISA RED Network
JWICS
DIA YELLOW Network
.GOV Networks
LAN-A
DMVPN
HSDN
DHS OneNet Black WAN Transport
Data Center #1 Component Networks
Data Center #2 Component Networks
HTSN
Campus Demarcation Points
.MIL
DEMARC-2
DEMARC-4
.GOV
DEMARC-2
DEMARC-4
Campus Fabric Layer
BLACK ROADM/DWDM Optical Fabric
Campus Core, Distribution, and Access Layers
Unclassified Networks
SBU
Classified Networks
SECRET
TS/SCI
* For brevity, only one classified network is being displayed on this diagram. The other classified network is identical.

Figure 1.2 St. Elizabeths Campus Physical Architecture - Legend



Represents HAIPE type-1 devices that are connected to the various .GOV and .MIL networks. These HAIPEs are only shown to articulate our level of understanding on on a high level how the different CoSMunity of Interests (CoIs) within the St.Es campus will coSMunicate to the .GOV and .MIL networks outside of the campus.

Campus IPT Connections:

AV = Audio Visual
EMS = Enterprise Management System
IA = Information Assurance
IPTV = Internet Protocol Television
PS = Physical Security
SF = Special Facilities

Figure 1.3 St. Elizabeths Campus Physical Architecture - Expanded View - Demarcation Points / Campus Fabric Layer

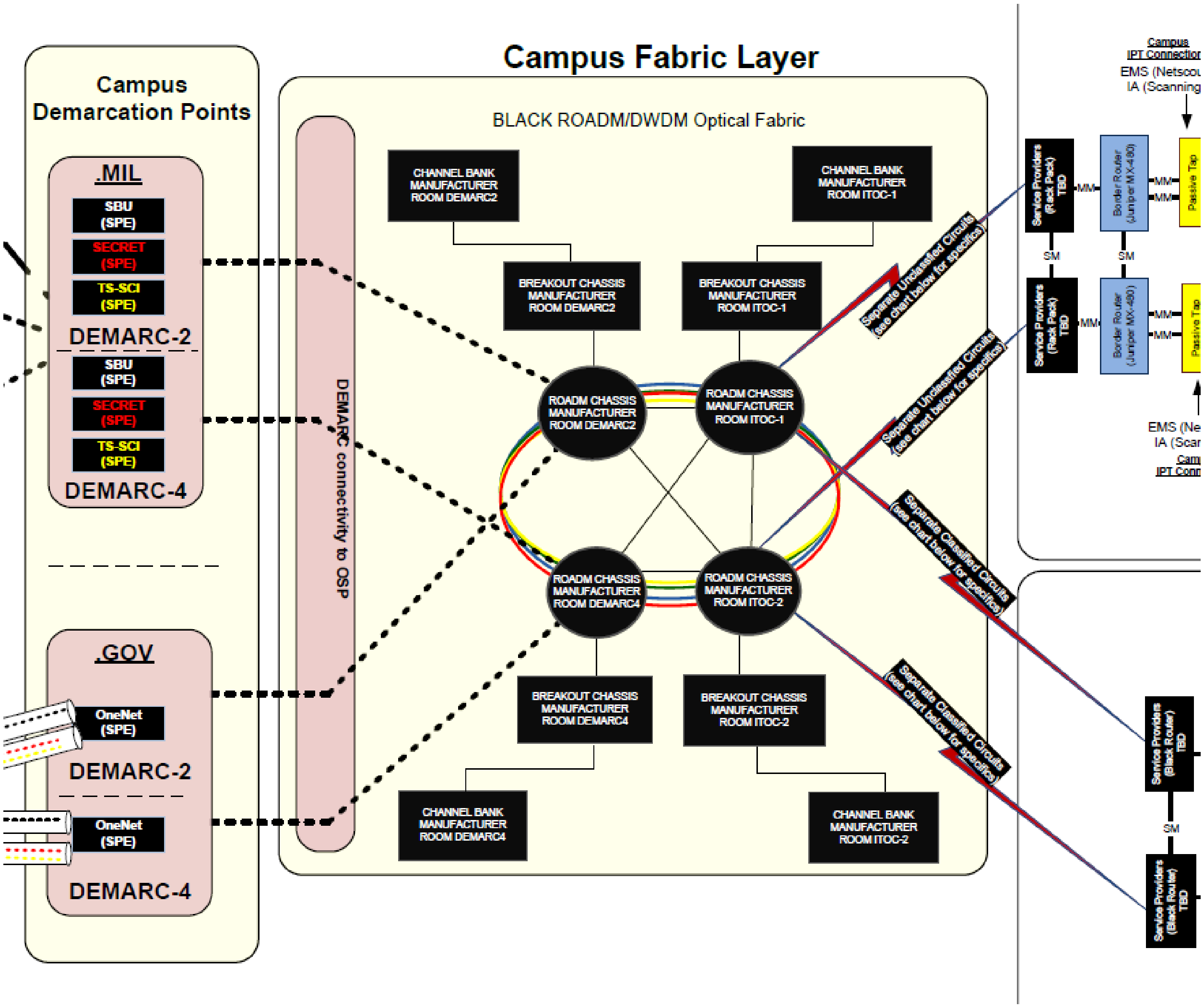
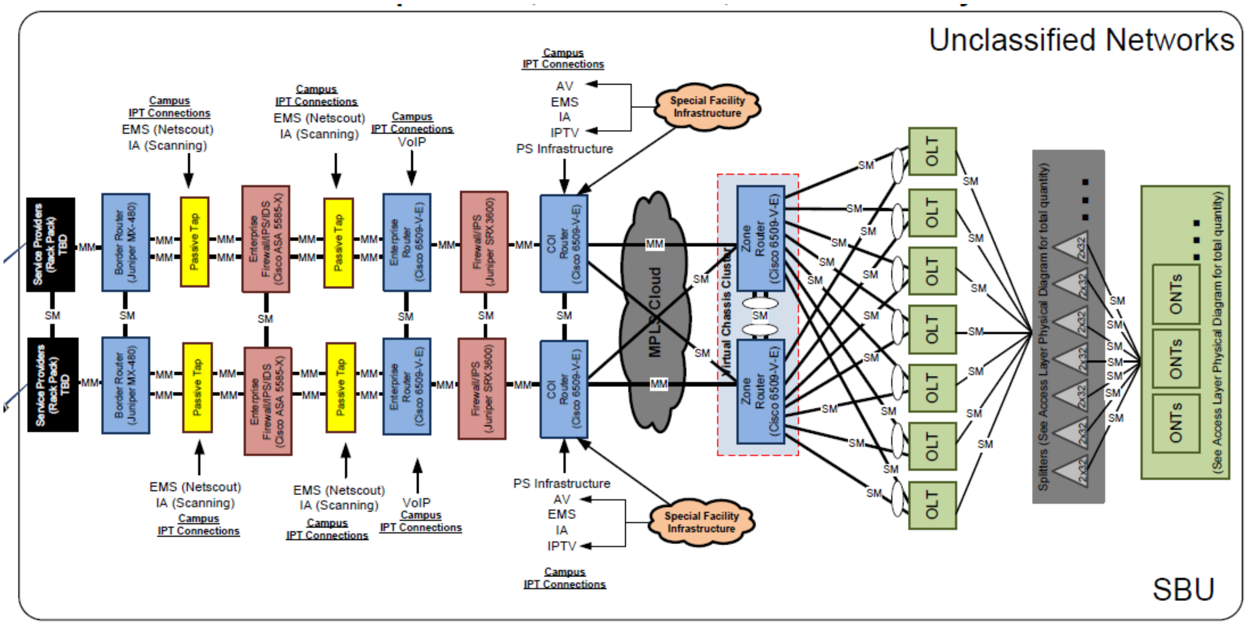
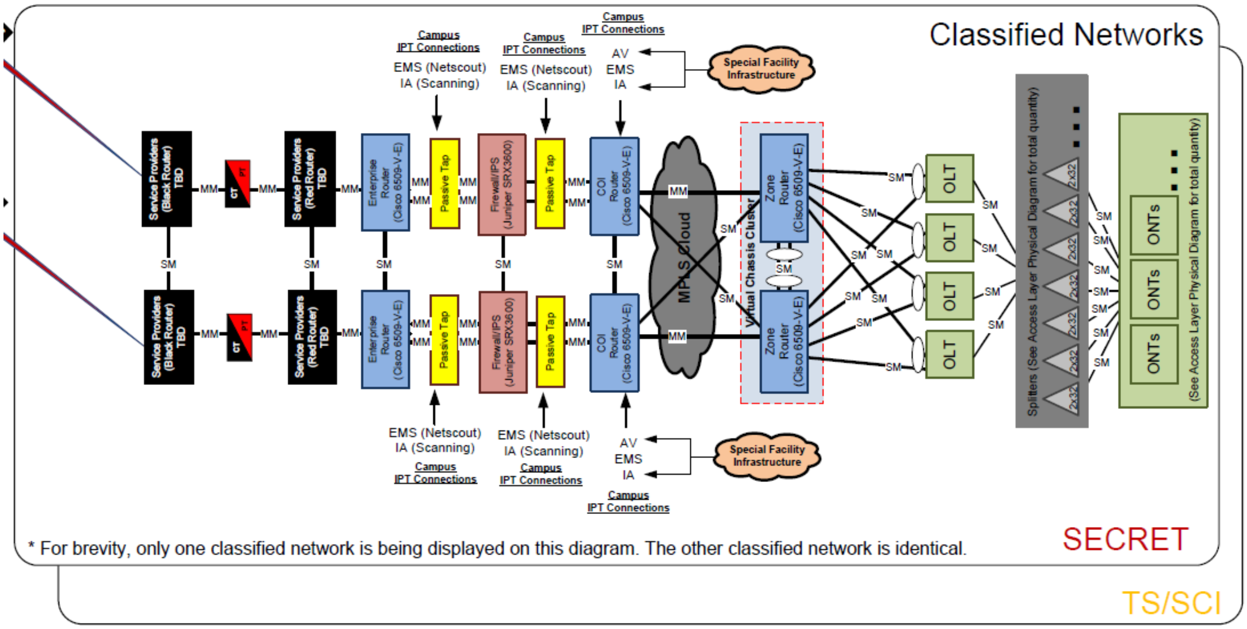

Campus Demarcation Points
.MIL
SBU (SPE)
SECRET (SPE)
TS-SCI (SPE)
DEMARC-2
SBU (SPE)
SECRET (SPE)
TS-SCI (SPE)
DEMARC-4
.GOV
OneNet (SPE)
DEMARC-2
OneNet (SPE)
DEMARC-4
Campus Fabric Layer
BLACK ROADM/DWDM Optical Fabric
DEMARC connectivity to OSP
CHANNEL BANK MANUFACTURER ROOM DEMARC2
CHANNEL BANK MANUFACTURER ROOM ITOC-1
BREAKOUT CHASSIS MANUFACTURER ROOM DEMARC2
BREAKOUT CHASSIS MANUFACTURER ROOM ITOC-1
ROADM CHASSIS MANUFACTURER ROOM DEMARC2
ROADM CHASSIS MANUFACTURER ROOM ITOC-1
ROADM CHASSIS MANUFACTURER ROOM DEMARC4
ROADM CHASSIS MANUFACTURER ROOM ITOC-2
BREAKOUT CHASSIS MANUFACTURER ROOM DEMARC4
BREAKOUT CHASSIS MANUFACTURER ROOM ITOC-2
CHANNEL BANK MANUFACTURER ROOM DEMARC4
CHANNEL BANK MANUFACTURER ROOM ITOC-2
Separate Unclassified Circuits (see chart below for specifics)
Separate Unclassified Circuits (see chart below for specifics)
Separate Classified Circuits (see chart below for specifics)
Separate Classified Circuits (see chart below for specifics)
Campus IPT Connection
EMS (Netscou
IA (Scanning
Service Providers (Rack Pack) TBD
MM
Border Router (Juniper MX-480)
MM
MM
Passive Tap
SM
SM
Service Providers (Rack Pack) TBD
MM
Border Router (Juniper MX-480)
MM
MM
Passive Tap
EMS (Ne
IA (Scan
Cam
IPT Conn
Service Providers (Black Router) TBD
SM
Service Providers (Black Router) TBD

Figure 1.4 St. Elizabeths Campus Physical Architecture - Expanded View - Unclassified Networks


Unclassified Networks
Campus IPT Connections
EMS (Netscout)
IA (Scanning)
VoIP
AV
EMS
IA
IPTV
PS Infrastructure
Special Facility Infrastructure
Service Providers (Rack Pack) TBD
Border Router (Juniper MX-480)
Passive Tap
Enterprise Firewall/IPS/IDS (Cisco ASA 5585-X)
Enterprise Router (Cisco 6509-V-E)
Firewall/IPS (Juniper SRX 3600)
COI Router (Cisco 6509-V-E)
MPLS Cloud
Virtual Chassis Cluster
Zone Router (Cisco 6509-V-E)
OLT
Splitters (See Access Layer Physical Diagram for total quantity)
2x32
ONTs
(See Access Layer Physical Diagram for total quantity)
MM
SM
SBU

The SBUCAN IT infrastructure also includes an Ethernet technology based topology (not pictured), in parallel with the GPON, that supports the St. Elizabeths Campus Physical Security services.

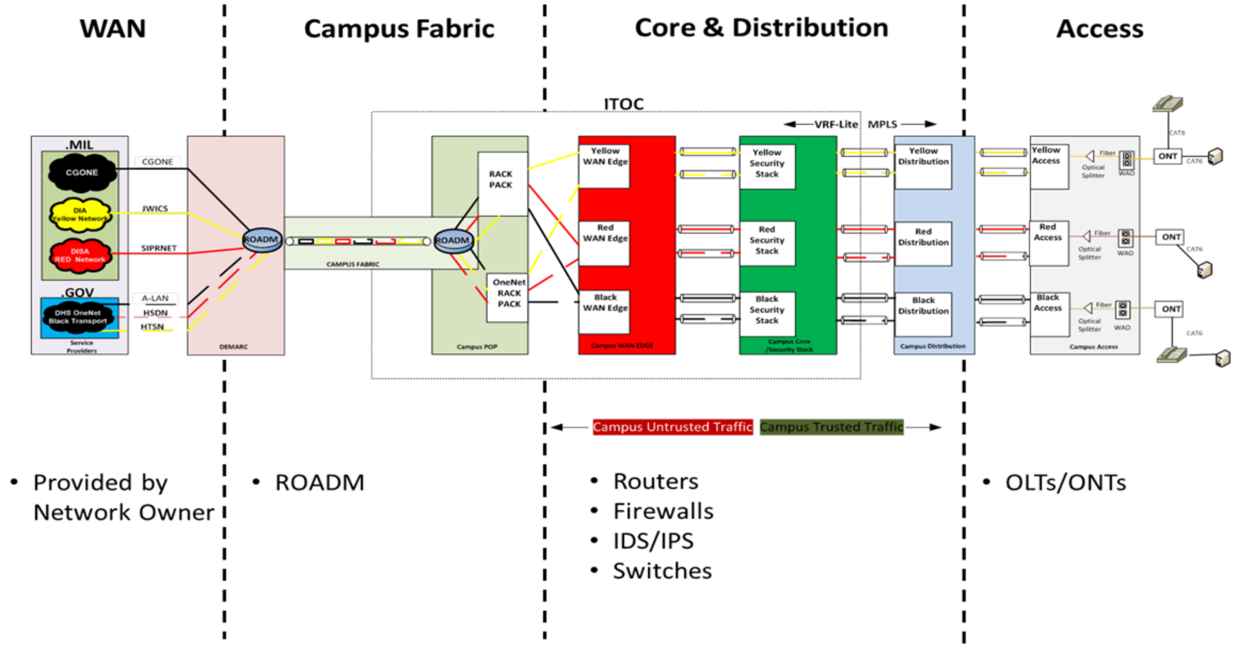
Figure 1.5 St. Elizabeths Campus Physical Architecture - Expanded View - Classified Networks


Classified Networks
Campus IPT Connections
EMS (Netscout)
IA (Scanning)
AV
EMS
IA
Special Facility Infrastructure
Service Providers (Black Router) TBD
Service Providers (Red Router) TBD
Enterprise Router (Cisco 6509-V-E)
Passive Tap
Firewall/IPS (Juniper SRX3600)
COI Router (Cisco 6509-V-E)
MPLS Cloud
Virtual Chassis Cluster
Zone Router (Cisco 6509-V-E)
OLT
Splitters (See Access Layer Physical Diagram for total quantity)
2x32
ONTs
(See Access Layer Physical Diagram for total quantity)
MM
SM
* For brevity, only one classified network is being displayed on this diagram. The other classified network is identical.
SECRET
TS/SCI

For SCAN and TSCAN IT infrastructures the GPON is secured inside Protective Distribution System (PDS).

Figure 2 further illustrates the St. Elizabeths Campus IT infrastructure. The St. Elizabeths Campus access layer utilizes GPON technologies to connect end devices to the St. Elizabeths Campus IT infrastructure, the distribution layer aggregates GPONs based on the density of end devices, building, and the expansion of the IT infrastructure, and the core layer performs high speed routing, switching, and network security functions.

Figure 2 St. Elizabeths Campus Core, Distribution, and Access Layer



The St. Elizabeths Campus IT infrastructure includes a limited number of Government-approved by exception, dedicated Point-To-Point (PTP) fiber connections from the St. Elizabeths Campus demarcation points to St. Elizabeths Campus facilities.

The St. Elizabeths Campus physical security services support the St. Elizabeths Campus life-safety requirements as set forth in the Risk Management Process for Federal Facilities Interagency Security Committee (ISC) Standards and Appendices (Section J, Attachment Tech-C).

GSA PBS construction and rehabilitation activities have and will continue to include pathways for vertical fiber, horizontal fiber, and copper and ladder racks as place holders for building and facilities IT infrastructure.

GSA PBS construction and rehabilitation activities have and will continue to include Outside Plant (OSP) utility tunnels and the direct burial of cable duct systems (e.g., conduit) for Fiber Optic Cables (FOC).

C.4 OBJECTIVES

The objective of the TO is to provide technical analysis, design, procurement, configuration, implementation, testing, securing, accrediting, and O&M of the St. Elizabeths Campus IT infrastructure to maintain business continuity and ensure mission support is successful during DHS Component Agency consolidation.

In supporting the preceding objective, the Government has identified the following technical objectives:

a. The St. Elizabeths Campus IT infrastructure conforms to Government (e.g., National Institute of Standards and Technology (NIST)), Organization, and Industry (e.g., Institute of Electrical and Electronics Engineers (IEEE)) Open Standards and Protocols (e.g., Internet Protocol (IP), IP Security (IPsec)).
b. The St. Elizabeths Campus IT infrastructure conforms to DHS Headquarters, Component Agencies, and other Government Agencies (e.g., Department of Defense (DoD), National Security Agency (NSA), and White House Communications Agency (WHCA)) architecture and operational standards and guidelines.
c. The St. Elizabeths Campus IT infrastructure applies System Engineering Life Cycle and Total Cost of Ownership (TCO) practices in the evaluation, selection, design, and O&M of IT systems and services.
d. The St. Elizabeths Campus IT infrastructure conforms to the technical philosophy of Everything over Internet Protocol (EoIP) to ensure the interoperability of communications between systems, services, and devices.
e. The procurement of COTS systems and services from third-party vendors with established product life-cycle support (e.g., software updates and security patches) to ensure the systems and services are commercially supported and sustained.
f. The St. Elizabeths Campus IT infrastructure limits the use of custom or non-standard IT systems and services solutions to mitigate interoperability risks and control life-cycle costs.
g. The procurement of IT systems and services to reduce utility costs (e.g., power, HVAC) and to support the Lead Energy and Environmental Design (LEED) Certifications.
h. O&M services for the St. Elizabeths Campus IT infrastructure follow Government and industry best practices and standards (e.g., Information Technology Infrastructure Library (ITIL)).

C.5 TASKS

The contractor shall provide IT services in compliance and conformance with the following for all tasks:

a. Department of Homeland Security Directives, Policies, and Guidelines:
   i. DHS 4300A Sensitive Systems Handbook (Section J, Attachment Tech-G).
   ii. DHS 4300B National Security Systems Policy Directive (Section J, Attachment Tech-H).
   iii. DHS 4300B.102 National Security Systems Security Control Guidance (Section J, Attachment Tech-N).
   iv. DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook (Section J, Attachment Tech-E).

v. DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle (Section J, Attachment Tech-F).

vi. DHS IT Security Architecture Guidance Volume 1 Network and System Infrastructure (Section J, Attachment Tech-X).

vii. DHS IT Security Architecture Guidance Volume 2 Security Operations and Support (Section J, Attachment Tech-Y).

viii. DHS IT Security Architecture Guidance Volume 3 Application Infrastructure Design (Section J, Attachment Tech-Z).

ix. DHS Infrastructure Change Control Board (ICCB) (Section J, Attachment Tech-I).

x. DHS Management Directive 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) (Section J, Attachment Tech-AA).

xi. DHS Management Directive 4300.1 Information Technology Systems Security (Section J, Attachment-Tech-BB).

xii. Homeland Security Enterprise Architecture (HLSEA) (Section H.3, GFI).

b. Federal Government Law, Regulations, and Policies:

i. Computer Security Act of 1987 (40 U.S.C. 1441 et seq.) (Publicly Available).

ii. Government Information Security Reform Act of 2000 (Publicly Available).

iii. FISMA of 2002 (Publicly Available).

iv. Federal policies and procedures include the Office of Management and Budget (OMB) Circular A-130 (Publicly Available).

v. National Historic Preservation Act (NHPA), Section 106 (Publicly Available).

c. Federal Government Standards and Publications:

i. GSA, Building Information Modeling (BIM) Guides (www.gsa.gov/bim).

ii. GSA, PBS CAD Standards (Section J, Attachment Tech-CC) (www.gsa.gov/cad).

d. Industry Standards and Publications:

i. International Standards Organization (ISO), ISO 16739: Industry Foundation Classes (IFC) for data sharing in the construction and facility management industries (Publicly Available).

ii. Internet Engineering Task Force (IETF) Internet Protocol, Version 6 (IPv6). Specification, Request For Comment (RFC) 2460 (Publicly Available).

iii. Institute of Electrical and Electronic Engineers (IEEE) 802.11 Wireless LANs (Publicly Available).

iv. National Institute of Building Sciences (NIBS), NIBS-United States Version 3: United States National Building Information Model Standard Procedures (Publicly Available).

v. NIST Special Publications (SP) 800 Series (Publicly Available).

vi. Underwriters Laboratories (UL) Standard for National Industrial Security Systems for the Protection of Classified Material, UL 2050 (Publicly Available).

e. Intelligence Community Directives, Policies, and Guidelines:

   i. Intelligence Community Standard Number 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (Section J, Attachment Tech-L).
   ii. Intelligence Community Standard Number 705-2 Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (Section J, Attachment Tech-M).
   iii. National Counterintelligence and Security Center Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Intelligence Community Directive (ICD) 705 (Section J, Attachment Tech-K).
   iv. Risk Management Process for Federal Facilities Interagency Security Committee (ISC) Standards and Appendices (Section J, Attachment Tech-C).

f. St. Elizabeths Campus Directives, Policies, and Guidelines:
   i. St. Elizabeths Information Technology Change Control Board (SEITCCB) (Section J, Attachment Tech-J).
   ii. St. Elizabeths Campus Operations and Maintenance Information Technology Service Provider Concept of Operations (CONOPS) (Section J, Attachment Tech-B).

g. United States Coast Guard Directives, Policies, and Guidelines:
   i. USCG Commandant Instructions (COMDT INST) 5503.13 (Commandant Information Assurance for .mil).

C.5.1 TASK 1 - TASK ORDER PROGRAM MANAGEMENT SERVICES

The contractor shall provide TO program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a TO Program Manager (TOPM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO. The contractor shall institute and maintain management and quality processes that ensure that the required TO performance is maintained or exceeded.

C.5.1.1 SUBTASK 1 – PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a **Project Kick-Off Meeting** (Section F, Deliverable 02). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, travel authorization and reporting procedures, and the delivery of Government-Furnished Information (GFI). At a minimum, the attendees shall include all contractor Key Personnel, DHS personnel, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR).

The contractor shall provide a **Kick-Off Meeting Agenda** in slide format (Section F, Deliverable 01) for review and approval by the FEDSIM COR and the DHS Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all TO tasks.
b. Status of the Program Management Plan (PMP) (Section C.5.1.4) with discussion of processes for managing schedule, costs, and risk.
c. Contractor organization overview (i.e., roles and responsibilities of the team, relationship between Government staff and corporate support resources, and a description of the lines of communication between the contractor and Government).
d. Updated Staffing Plan with skill matrix identification of required security clearance level.
e. Final Transition-In Plan discussion (Section C.5.6.1).
f. Security discussion and requirements (e.g., St. Elizabeths Campus building access, DHS Personal Identity Verification (PIV) cards, Entry on Duty (EOD) status).
g. Charge code management and invoicing considerations.
h. Project Reporting.

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a **Kick-Off Meeting Minutes Report** (Section F, Deliverable 03) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 2 – MONTHLY STATUS REPORT (MSR)

The contractor’s TOPM shall develop and provide a **Monthly Status Report (MSR)** (Section F, Deliverable 05). At a minimum, the MSR shall include the following:

a. Activities during reporting period, by task (e.g., on-going activities, new activities, activities completed; long-distance travel, progress to date on all above mentioned activities).
b. SLA and Metrics Monthly Report to include issues, concerns, and proposed resolutions for missed SLAs and metrics.
c. Problems and corrective actions taken.
d. Risks at the program level and project level with mitigation plans.
e. Personnel gains, losses, and status.
f. Government actions required.
g. Security status of contractor personnel including security clearance adjudication.

C.5.1.3 SUBTASK 3 – TECHNICAL STATUS MEETINGS

The contractor’s TOPM shall convene **Technical Status Meetings** (Section F, Deliverable 06) with the DHS TPOC, FEDSIM COR, and Government Program Management Offices (PMOs) as required during the TO’s period of performance. The purpose of these meetings is to ensure all stakeholders are informed of the activity and status, provide opportunities to identify missing or required activities and establish priorities, and coordinate resolution of identified problems or opportunities. The TOPM shall provide minutes of these meetings (i.e., **Technical Status Meeting Minutes** (Section F, Deliverable 07)), including attendance, issues discussed, decisions made, and action items assigned, to the Government.

C.5.1.4 SUBTASK 4 – PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a Program Management Plan (PMP). The contractor shall provide the Government with a **PMP** (Section F, Deliverable 08) on which the Government will make comments. The PMP is an evolutionary document. The contractor shall work from the latest Government-approved version of the PMP which includes, as Attachments, the latest Quality Management Plan (QMP) and Configuration Management Plan (CMP).

The PMP shall:

a. Describe the management methodology.
b. Describe the management systems, services, applications, and tools (e.g., Microsoft (MS) Project).
c. Describe the configuration management and change management methodology.
d. Describe the methodology for identifying and managing projects.
e. Describe the methodology for managing cost and schedule (e.g., Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS)).
f. Describe the methodology for coordinating communications and responsibilities between the contractor and the Government.
g. Describe the methodology for identifying risks and mitigating risks at both the program level and the project level.
h. Describe the methodology for quality management and quality control.

C.5.1.5 SUBTASK 5 – QUALITY MANAGEMENT PLAN (QMP)

The contractor shall provide a **Quality Management Plan (QMP)** (Section F, Deliverable 10) describing how it shall ensure quality management throughout the TO. The QMP shall identify and describe how the contractor shall comply with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, DHS 4300A Sensitive Systems Handbook, DHS 4300B National Security Systems Policy Directive, and other industry and Government quality management best practices. The contractor shall establish the infrastructure, support organizations, processes, tools, and procedures to implement the QMP.

C.5.1.6 SUBTASK 6 – DATA AND DELIVERABLES MANAGEMENT

The contractor shall utilize a Government-provided enterprise electronic Project Management (e-PM) system (Proliance software) (Section H.3, Government-Furnished Information (GFI)). e-PM is an internet-based information and project communication system that allows the St. Elizabeths' project team (e.g., GSA PBS, GSA FEDSIM, DHS, and all construction contractors) to collaborate in a centralized and secured Government repository. The contractor shall store and route within the e-PM system all construction-related communications and artifacts with GSA PBS and construction contractors, workflow processes, and documentation that is required for Other Government Contractors (OGC) activities on the St. Elizabeths Campus.

The contractor will be provided usernames and passwords after contractors have completed the Homeland Security Presidential Directive-12 (HSPD-12) process. The contractor shall log into the e-PM system to enter the Project Documentation listed in the bulleted list below. GSA PBS will hold training sessions to familiarize contractor staff (e.g., project control personnel) with the e-PM system.

In accordance with Section F.5, the contractor shall post, store, and maintain all deliverables and all documentation produced pursuant to this TO on a DHS-furnished and hosted/contractor-maintained DHS SharePoint Portal that will be provided as GFI after TOA (Section H.3, GFI).

In addition, the contractor shall post, in a timely and accurate manner, review, respond, and collaborate with OGCs using the following features and/or workflow processes within both the e-PM and DHS SharePoint systems:

a. Project Team Directory – The contractor shall provide an updated directory of contact information in accordance with the contractor’s Communication Plan.
b. Schedules – The contractor shall post, review, and/or respond to schedule updates and shall receive and incorporate schedule updates from OGCs.
c. Design Drawings/Design Packages – The contractor shall submit design drawings and design packages into both systems and receive design drawings and design packages from OGCs via e-PM.
d. Punch lists – Maintain list(s) of observed defects and omissions.
e. Issue Tracking – The contractor shall log and respond to issues.
f. Requests for Information (RFI) – The contractor shall enter RFIs from OGCs into the e-PM system and will respond to RFIs from OGCs in the e-PM system. An RFI log will be maintained in the DHS SharePoint system.

The Government will facilitate initial contact between the contractor and OGCs performing work for GSA or DHS. The contractor shall provide support services to OGCs within the scope of this TO as required by the Government. The contractor shall notify the designated representative in writing of unresolved disputes in receiving support from or providing support to customers or OGCs within two business days from the time the dispute occurs.

C.5.1.7 SUBTASK 7 – RISK MANAGEMENT

The contractor shall provide a systematic structured, formalized, forward thinking, flexible, adaptable, and continuous process to risk management for the TO. The contractor’s risk management process shall be a value-based systematic process to managing all risks from all sources to improve the contractor’s performance in meeting TO requirements. The contractor shall use the best industry and Government practices to develop, implement, and manage, on an ongoing basis, the risk management process. The risk management process (included in the PMP) shall provide clear visibility into program risks in the areas such as scope, costs, schedule, and technical performance. At a minimum, the contractor shall track risks, risk levels, risk impacts, risk mitigations, and risks that have become issues in the MSR.

C.5.1.8 SUBTASK 8 – FINANCIAL MANAGEMENT

The contractor shall comply and execute financial management in accordance with the DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, the DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, and other industry and Government financial management best practices (e.g., Project Management Body of Knowledge (PMBOK), ITIL, PRojects IN Controlled Environments (PRINCE2)).

The Government will assign "project" status to specific St. Elizabeths Campus IT infrastructure activities based on technical (e.g., system boundaries and security boundaries), operational, organizational, and funding source (e.g., Federal Protective Service (FPS) and DHS) demarcations under:

a. Task 2 - Requirements Analysis and Design Services
b. Task 3 - Implement, Test, and Secure Services
c. Task 4 - Operations and Maintenance Services
d. Task 5 - IT Infrastructure Transitional Services

The Government may assign "project" status to additional St. Elizabeths Campus IT infrastructure activities under:

a. Task 6 - Task Order Transition Support Services

The contractor may define additional "projects" as applicable under:

a. Task 1 - Task Order Program Management Services
b. Task 4 - Operations and Maintenance Services
c. Task 5 - IT Infrastructure Transitional Services
d. Task 6 - Task Order Transition Support Services

The contractor shall coordinate and synchronize financial management with schedule management reporting and deliverables.

The contractor shall develop and maintain a St. Elizabeths Campus IT Infrastructure **Financial Management Report** (Section F, Deliverable 11).

The St. Elizabeths Campus IT Infrastructure Financial Management Report shall include the following minimum information and data for all CLINs:

a. CLIN Number / Title.
b. CLIN Ceiling Amount.
c. CLIN Funded Amount.
    i. Cost (as applicable)
    ii. Fee (as applicable)
d. CLIN Last Funding Action (i.e., Modification Number).
e. CLIN Estimated Costs.
f. CLIN Incurred Costs to Date.
g. CLIN Delta between Estimated Costs and Funded Costs.
h. CLIN Delta between Funded Costs and Incurred Costs.
i. CLIN Percentage of Funded Costs vs Incurred Costs.
j. CLIN Estimated Burn Rate Trajectory (e.g., decreasing, steady, increasing).

The St. Elizabeths Campus IT Infrastructure Financial Management Report shall include the following minimum information and data for all "projects" under the appropriate CLIN:

a. Project Number / Title.
b. Project Task Number (i.e., Tasks 1, 2, 3, 4, 5, 6).

c. Project Estimated Costs, Government-Approved Amount.
d. Project Estimated Costs, Government-Approved Version / Date.
e. Project Funded Amount.
    i. Cost (as applicable)
    ii. Fee (as applicable)
f. Project Last Funding Action (i.e., Modification Number, Technical Direction Letter).
g. Project Estimated Costs.
h. Project Incurred Costs to Date (i.e., cumulative).
i. Project Incurred Costs Correlated to IMS Milestones (e.g., deliverables).
j. Project Delta between Estimated Costs and Funded Costs.
k. Project Delta between Funded Costs and Incurred Costs.
l. Project Percentage of Funded Costs versus Incurred Costs.
m. Project Estimated Burn Rate Trajectory (e.g., decreasing, steady, increasing).
n. Project Estimated Date of when Funded Cost equals Incurred Costs.

The contractor shall convene a St. Elizabeths Campus IT Infrastructure **Financial Management Report Review** (Section F, Deliverable 12) with the Government. The Financial Management Report Review is a meeting for the contractor and the Government to mutually review and discuss the Financial Management Report.

The contractor shall deliver **Financial Management Report Review Minutes** (Section F, Deliverable 13) after each Financial Management Report Review.

C.5.1.8.1 GOVERNMENT REQUEST FOR COST ESTIMATE

The contractor shall deliver St. Elizabeths Campus IT Infrastructure **Cost Estimates** (Section F, Deliverable 14) to the Government in response to a Government Request for Cost Estimate (GRFCE). A GRFCE workflow is provided as a TOR Attachment (Section J, Attachment Tech-D).

The Cost Estimates shall include as a minimum the following sections:

a. Scope of Work.
b. Contractor Assumptions.
c. Contractor Limitations or Restrictions.
d. Basis of Estimate Narrative.
e. Cost Estimate per TO Task (e.g., Task 2, Task 3, Tools).
    i. Identification of Cost Reserves per TO Task.
    ii. Identification of Cost Risks per TO Task.
f. Notional Schedule.
g. Identification of Schedule Risks.
h. Identification of Long Lead Time Tools.

C.5.1.9 SUBTASK 9 – SCHEDULE MANAGEMENT

The contractor shall comply and execute in accordance with the DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, the DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, and other industry and Government schedule management best practices (e.g., PMBOK, ITIL, and PRINCE2) in the execution of schedule management.

The Government will assign "project" status to specific St. Elizabeths Campus IT infrastructure activities based on technical (e.g., system boundaries and security boundaries), operational, organizational, and funding source (e.g., FPS, DHS) demarcations under:

a. Task 2 - Requirements Analysis and Design Services.
b. Task 3 - Implement, Test, and Secure Services.
c. Task 4 - Operations and Maintenance Services.
d. Task 5 - IT Infrastructure Transitional Services.

The Government may assign "project" status to additional St. Elizabeths Campus IT infrastructure activities under:

a. Task 6 - Task Order Transition Support Services.

The contractor may define additional "projects" as applicable from:

a. Task 1 - Task Order Program Management Services.
b. Task 4 - Operations and Maintenance Services.
c. Task 5 - IT Infrastructure Transitional Services.
d. Task 6 - Task Order Transition Support Services.

The contractor shall coordinate and synchronize schedule management with financial management reporting and deliverables.

The contractor shall develop and maintain a St. Elizabeths Campus IT Infrastructure **Integrated Master Schedule** (IMS) (Section F, Deliverable 15).

The St. Elizabeths Campus IT Infrastructure IMS shall include the following minimum information and data for all Government-assigned "projects":

a. Project Name / Number
    i. Project Tasks and Sub-Tasks aligned with Project WBS:
        a. Planned Start Date, Duration, and End Date
        b. Actual Start Date, Duration, and End Date
        c. Predecessors and Successors
        d. Percent Complete
        e. Estimated Level of Effort (LoE) (e.g., work hours)
        f. Resource Loaded by Labor Category
        g. Planned Costs
        h. Actual Costs
    ii. Project Milestones:

        a. System Definition Reviews (as applicable)
        b. Preliminary Design Reviews (as applicable)
        c. Critical Design Reviews (as applicable)
        d. Operational Readiness Reviews (ORRs) (as applicable)
        e. Tenant Move-In (TMI) (as applicable)

iii. TO Milestones:

    a. TO Period of Performance
    b. CLINs Period of Performance

iv. Project External Dependencies:

    a. Construction Schedules
    b. Service Providers (e.g., connectivity)
    c. DHS Component Agency Activities
    d. Long Lead Time Items (e.g., tools, encryption devices)

The St. Elizabeths Campus IT Infrastructure IMS shall include the following minimum capabilities:

a. Identify Critical Paths at the:
    i. Project Level
    ii. IMS Level
b. Identify Critical Paths Variance at the:
    i. Project Level
    ii. IMS Level
c. Identify Schedule Risk at the:
    i. Project Level
    ii. IMS Level
d. Identify Resource Allocation at the:
    i. Project Level
    ii. IMS Level
e. Identify Resource Utilization at the:
    i. Project Level
    ii. IMS Level

The contractor shall convene an **IMS Review** (Section F, Deliverable 16) with the Government. The IMS Review is a meeting for the contractor and the Government to mutually review and discuss the IMS.

The contractor shall deliver **IMS Review Minutes** (Section F, Deliverable 17) after each IMS Review.

C.5.1.10 SUBTASK 10 – LOGISTICS MANAGEMENT

The contractor shall develop, implement, and maintain an **Integrated Logistics Support Plan (ILSP)** (Section F, Deliverable 61). The ILSP shall identify and describe the processes and procedures of how the contractor shall satisfy schedules (e.g., IMS and projects) and meet or exceed SLAs, comply with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, DHS Directives Systems Directive Number 119-03 Personal Property Management, and other industry and Government logistical services best practices.

C.5.1.11 SUBTASK 11 – TRIP REPORTS

The Government will identify the need for a **Trip Report** (Section F, Deliverable 18) when a **Travel Authorization Request (TAR)** (Section J, Attachment H) is submitted to the Government. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip Reports shall also contain Government approval authority, total cost of the trip, and a detailed description of the purpose of the trip. The contractor shall report knowledge obtained in the DHS SharePoint. The contractor shall prepare Trip Reports in accordance with Section J, Attachment G.

C.5.2 TASK 2 - REQUIREMENTS ANALYSIS AND DESIGN SERVICES

The contractor shall use a systems engineering methodology to conduct requirements analysis and design for the St. Elizabeths Campus IT infrastructure that includes the collection, refinement, and validation of IT infrastructure requirements for technical feasibility, proficiency, quality, integration and interoperability, costs, and compliance with Government architectures, standards, design guides, and policies.

The contractor shall conduct requirements analysis and design for new and existing St. Elizabeths Campus IT infrastructure as documented in the Engineering Implementation Plans (EIPs) and CONOPS.

The contractor shall use a systems engineering methodology to design (i.e., engineer) technical solutions for the St. Elizabeths Campus IT infrastructure that meet or exceed the Governments' approved requirements that are technically feasible, proficient, integrated, and interoperable and in compliance with Government architectures, standards, design guides, and policies.

The Government will approve the contractor's requirements and analysis and design for St. Elizabeths Campus IT infrastructure equipment, technology, and solutions using the following:

a. HLSEA Technical Reference Model (TRM) Standards and Products Profiles (Section H.3, GFI).
b. Where applicable, the DHS Enterprise Architecture Information Repository.
c. Where applicable, certified under the National Information Assurance Partnership (NIAP) Common Criteria.
d. Where applicable, certified under the Federal Information Processing Standards (FIPS).
e. Where applicable, certified by the Joint Interoperability Test Command (JITC).
f. Where applicable, the Department of Defense (DoD) Unified Capabilities (UC) Approved Product List (APL).
g. Where applicable, the Federal Identity, Credential, and Access Management (FICAM) Physical Access Control System (PACS) APL.

When the contractor recommends IT infrastructure equipment, technology, and solutions that are not Government approved or do not comply with Government, organization, or industry standards and protocols the contractor shall:

a. Comply with all policies and procedures for the introduction of new equipment, technology, and solutions per:

    i. Certification and Authorization (C&A).

    ii. Authorization To Operate (ATO).

    iii. HLSEA TRM.

    iv. DHS Enterprise Architecture Information Repository.

b. Coordinate with DHS Management (MGMT)/OCIO/Information Technology Services Office (ITSO)/Enterprise Data Management Office (EDMO) through the ITSO/Customer Relationship Management Division (CRMD)/St. Elizabeths Special Program Office.

c. Coordinate with the DHS and St. Elizabeths Campus IT infrastructure Governance Boards.

C.5.2.1 SUBTASK 1 - REQUIREMENTS ANALYSIS AND DESIGN MANAGEMENT

The contractor shall comply and execute in accordance with the DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, the DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, and other industry and Government systems engineering best practices (e.g., PMBOK, ITIL, and PRINCE2).

The Government will assign “project” status to requirements analysis and design activities for the St. Elizabeths Campus IT infrastructure based on technical (e.g., system boundaries and security boundaries), operational, or organizational demarcations. The Government will organize projects into an overarching St. Elizabeths Campus IT infrastructure portfolio.

In support of the St. Elizabeths Campus IT infrastructure portfolio, the contractor shall, for each project:

a. Develop and manage to project plans.
b. Develop and manage to project WBSs.
c. Develop and manage to project schedules.
d. Develop and manage to costs.
e. Identify and manage to risks and issues.
f. Identify, coordinate, and manage requirement analysis and design activities with contractor personnel, Government personnel, and other Government contractors.
g. Identify, coordinate, and manage communications (e.g., technical, schedules, and risks) with contractor personnel, Government personnel, and other Government contractors.
h. Identify, coordinate, and manage the reporting of project status with contractor personnel, Government personnel, and other Government contractors.

The contractor shall develop a St. Elizabeths Campus **IT Infrastructure Engineering Master Plan** (Section F, Deliverable 19). The St. Elizabeths Campus IT Infrastructure Engineering

Master Plan shall identify and describe how the contractor shall comply with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, DHS 4300A Sensitive Systems Handbook, DHS 4300B National Security Systems Policy Directive, and other industry and Government systems engineering best practices.

C.5.2.2 SUBTASK 2 - INFORMATION TECHNOLOGY (IT) INFRASTRUCTURE

C.5.2.2.1 IT ARCHITECTURE

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure. The contractor shall assess and document the impact to existing IT infrastructure and technology O&M as part of the design process.

The contractor, in coordination with the Government, may recommend alternative IT infrastructure equipment, technologies, and solutions that improve (e.g., capabilities, performance, and integration) of the St. Elizabeths Campus IT infrastructure.

C.5.2.2.1.1 CAMPUS FABRIC

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Fabric. The St. Elizabeths Campus Fabric is comprised of ROADMs.

C.5.2.2.1.2 CAMPUS GIGABIT PASSIVE OPTICAL NETWORK (GPON)

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus GPON. The St. Elizabeths Campus GPON is comprised of Optical Line Terminals (OLTs) and Optical Network Terminals (ONTs)/ Optical Network Units (ONUs).

C.5.2.2.1.3 CAMPUS AND BUILDING OUTSIDE PLANT (OSP) WIRING

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus and building OSP wiring. The St. Elizabeths Campus and building OSP wiring is comprised of utility tunnels, direct buried conduit, and FOCs.

GSA PBS will be responsible for the installation of OSP utility tunnels and the direct burial of cable duct tubing (e.g., conduit).

The contractor shall provide St. Elizabeths Campus and building OSP wiring design requirements to GSA PBS. The contractor shall provide recommendations for OSP infrastructure (e.g., cables and conduit) that will support the St. Elizabeths Campus IT infrastructure.

C.5.2.2.1.3.1 DEDICATED POINT-TO-POINT (PTP) WIRING

The contractor shall perform requirements analysis and design to develop, expand, and extend dedicated point-to-point (PTP) wiring (e.g., fiber) connections from the St. Elizabeths Campus demarcation points to St. Elizabeths Campus facilities.

C.5.2.2.1.4 CAMPUS AND BUILDING INSIDE PLANT (ISP) WIRING

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus and building Inside Plant (ISP) wiring. The St. Elizabeths Campus and building ISP wiring comprises of fiber strands, FOCs, and Ethernet cables.

GSA PBS will be responsible for the installation of pathways for vertical fiber, horizontal fiber, and copper and ladder racks for building and facilities IT infrastructure.

The contractor shall provide St. Elizabeths Campus and building ISP wiring design requirements to GSA PBS. The contractor shall provide recommendations for ISP infrastructure (e.g., fiber and Ethernet) that will support the St. Elizabeths Campus IT infrastructure.

C.5.2.2.1.5 UNINTERRUPTIBLE POWER SUPPLY (UPS)

The contractor shall perform requirements analysis and design of the St. Elizabeths Campus IT infrastructure for backup power using Uninterruptible Power Supplies (UPS).

C.5.2.2.1.6 INTERNET PROTOCOL (IP) ADDRESSING

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure Internet Protocol (IP) addressing (e.g., private, public, non-routable, and routable).

C.5.2.2.1.7 LOGICAL PARTITIONING

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure logical partitioning (e.g., Multiprotocol Label Switching (MPLS) and VLAN).

C.5.2.2.1.7.1 INTERNET ONLY ACCESS LOCAL AREA NETWORK (I-LAN)

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus IT infrastructure to provide a logical partition for DHS Internet Only Access Local Area Network (I-LAN).

C.5.2.2.1.7.2 NON-DHS COMPONENT AGENCIES AND COMMERCIAL VENDORS

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus IT infrastructure to provide logical partitions for non-DHS Component Agencies and commercial vendors.

C.5.2.2.2 DEMARCATION POINTS

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus demarcation points. The St. Elizabeths Campus demarcation points (i.e., facilities) provide geographical diverse and redundant connectivity to Government and commercial (e.g., telecommunication carriers) Wide Area Networks (WANs). The St. Elizabeths Campus demarcation points provide the only wired connectivity (e.g., touch points, interfaces, and interconnects) between the St. Elizabeths Campus IT infrastructure and off-Campus Government services (e.g., WANs, internet, and networks). There are two existing telecommunications demarcation points located on the St. Elizabeths Campus.

The contractor shall provide recommendations for Government services connectivity (e.g., bandwidth) that will support the St. Elizabeths Campus IT infrastructure. The contractor shall coordinate (e.g., configure and secure) with the Government services PMOs to provide Government services connectivity to the St. Elizabeths Campus.

C.5.2.2.2.1 OFF-CAMPUS DATA CENTER (DC) CONNECTIVITY

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus connectivity to remote Data Centers (DCs) via Government services (e.g., WANs).

The DHS operates two DCs. DC-1, also called the National Center for Critical Information Processing and Storage (NCCIPS), is located at the John C. Stennis Space Center (SSC) in Mississippi. DC-2 is located in Clarksville, Virginia. DC-1 and DC-2 are implemented and operated in a redundant configuration. Connectivity to DC-1 and DC-2 are provided via DHS WANs.

The USCG operates a DC in Clarksburg, West Virginia. Connectivity to the USCG DC is provided via DoD WANs.

The contractor shall provide recommendations for DC connectivity (e.g., bandwidth) that will support the St. Elizabeths Campus IT infrastructure. The contractor shall coordinate (e.g., configure, secure) with the Government to provide DCs connectivity to the St. Elizabeths Campus.

C.5.2.2.2.2 OFF-CAMPUS CONNECTIVITY

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus connectivity to Government services (e.g., WAN). The contractor shall provide recommendations for connectivity (e.g., bandwidth) that will support the St. Elizabeths Campus IT infrastructure. The contractor shall coordinate (e.g., configure and secure) with PMOs to provide connectivity to the St. Elizabeths Campus.

C.5.2.2.2.3 OFF-CAMPUS REMOTE SATELLITE CONNECTIVITY

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus connectivity to receive remote satellite data feeds.
Remote satellite data feeds shall connect to the St. Elizabeths Campus IT infrastructure via the St. Elizabeths Campus demarcation points.

C.5.2.2.3 RADIO FREQUENCY (RF) MOBILITY SERVICE

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Radio Frequency (RF) mobility services. Requirements analysis and design is inclusive of conducting RF studies (e.g., coverage, strength and propagation) to ensure technical feasibility, proficiency, quality, integration, and interoperability of RF mobility services with the St. Elizabeths Campus IT infrastructure.

The contractor shall comply with Section 106 of the National Historic Preservation Act (NHPA), which controls the use, size, quantities, and locations of external and internal antennas, equipment, and other required RF mobility services. The contractor shall comply with all

Government requirements for the proximity of RF mobility services infrastructure (e.g., antennas, coverage area, and wave propagation) to Sensitive Compartmented Information Facility (SCIF) or other Government-designated areas.

C.5.2.2.3.1 MOBILE WIRELESS COMMUNICATION SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus mobile wireless communication services.

The contractor shall coordinate with commercial mobile wireless communication services to provide connectivity to the St. Elizabeths Campus IT infrastructure and the commercial mobile wireless communication services equipment. Currently Verizon, AT&T, and T-Mobile provide mobile wireless communication services on the St. Elizabeths Campus. Commercial mobile wireless communication services include cellular, Personal Communications Service (PCS), Long-Term Evolution (LTE), and Advanced Wireless Services (AWS). The commercial mobile wireless communications providers are responsible for the installed head-in commercial equipment (e.g., O&M services).

C.5.2.2.3.2 LAND MOBILE RADIO (LMR)

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Land Mobile Radio (LMR) services. St. Elizabeths Campus LMR services support DHS life-safety, emergency, and security services (e.g., communications) and personnel (e.g., FPS) across the St. Elizabeths Campus to include buildings, pedestrian tunnels, parking garages, and open spaces. The St. Elizabeths Campus LMR services shall operate in both the Ultra High Frequency (UHF) and Very High Frequency (VHF) spectrums, provide encrypted and non-encrypted communications, and integrate and interoperate with Emergency (“E”), DHS, Federal, state, and local municipalities LMR services.

The contractor shall coordinate (e.g., integrate and configure) with DHS, Federal, state, and local municipalities to provide LMR services on the St. Elizabeths Campus.

C.5.2.2.3.3 WIRELESS SERVICES

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus wireless services (i.e., Wireless Fidelity (Wi-Fi)).

The wireless services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure, to include physical isolation (e.g., physical IT infrastructure) and logical partitioning (e.g., VLAN).

The wireless services design shall only allow authorized access (e.g., Government users, authorized guests) and provide seamless mobility between wired and wireless connections with location identification services.

C.5.2.2.3.4 WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus Wireless Intrusion Detection System (WIDS) services. The WIDS services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure (e.g., wireless services) and be certified under the NIAP Common Criteria and approved by the authorized Government Delegated Approving Authority (DAA).

The WIDS services design shall at a minimum provide the following:

a. Continuous monitoring (i.e., 24 hours a day, 7 days a week, and 365 days a year (24x7x365)) of the St. Elizabeths Campus wireless services for detection of attempted intrusions and intrusions of the St. Elizabeths Campus IT infrastructure.
b. Continuous scanning (i.e., 24x7x365) for and detection, reporting, and mitigation of unauthorized activities.
c. Location identification and reporting capabilities that determine the location of attempted intrusions and intrusions of the St. Elizabeths Campus IT infrastructure.
d. An independent and isolated antenna system from the St. Elizabeths Campus wireless services.
e. Provide for the following defensive capabilities:
    i. RF surveillance of IEEE 802.11 2.4 GHz and 5 GHz frequency ranges and channels.
    ii. Detection of known vulnerabilities (e.g., signature-based).
    iii. Anomaly-based threat detection.
    iv. Detection of rogue wireless access point (AP) discovery.
    v. Detection of authorized and unauthorized clients/devices.
    vi. Detection and assessment of DHS security policy deviations.
    vii. Physical location awareness of wireless devices.
    viii. Interference detection and spectrum analysis.
    ix. Mobile ad hoc network detection and packet and forensic analysis of wireless traffic.

C.5.2.2.3.5 SATELLITE COMMUNICATION SERVICES

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus satellite communication services. The satellite communication services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure. St. Elizabeths Campus historical property restrictions do not allow for an extensive or significant satellite dish or antenna facility.

The satellite communication services design shall provide the following:

a. Connectivity via the St. Elizabeths IT infrastructure to all demarcation points providing redundant means for establishing St. Elizabeths Campus Off-Campus connections (e.g., DCs, DHS OneNet, and Defense Information Systems Network (DISN)).
b. Connectivity to the St. Elizabeths Campus Mobile Satellite Connection Facility.
c. Connectivity for a minimum of three mobile satellite communication vehicles at the Mobile Satellite Connection Facility.
d. Connectivity for approximately two satellite dishes to be located in proximity to the Central Utility Plant (CUP).
e. Connectivity for radios, microwave antennas, and iridium phones.

The contractor shall provide requirements for electrical power at the Mobile Satellite Connection Facility that will support the St. Elizabeths Campus IT infrastructure and mobile satellite communication vehicles to GSA PBS.

C.5.2.2.3.6 SECURE POINT–TO-POINT (PTP) HIGH-SPEED WIRELESS SERVICES

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus secure Point-To-Point (PTP) high-speed wireless services.

The secure PTP high-speed wireless services (e.g., free space optics, millimeter wave technologies) design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure and provide connectivity via the St. Elizabeths IT infrastructure to all demarcation points providing redundant means for establishing St. Elizabeths Campus Off-Campus connections (e.g., DCs, DHS OneNet, DISN) within the NCR.

The contractor shall provide recommendations for secure PTP high speed wireless services connectivity (e.g., bandwidth) that will support the St. Elizabeths Campus IT infrastructure.

The contractor shall coordinate (e.g., configure, secure) with the Government to provide secure PTP high-speed wireless services connectivity to the St. Elizabeths Campus.

C.5.2.2.4 SHARED SERVICES BACK-END SYSTEMS

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure shared services back-end systems.

C.5.2.2.4.1 VOICE OVER INTERNET PROTOCOL (VoIP)

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Voice over Internet Protocol (VoIP) back-end systems.

The St. Elizabeths Campus VoIP back-end system uses open and industry standard Session Initiation Protocol (SIP), Secure SIP, and virtual Private Branch Exchange (PBX) capabilities.

The VoIP back-end system shall support multiple dialing plans (e.g., numbering plans) to support multiple DHS Component Agencies.

The contractor shall provide recommendations for dialing plans that will support DHS Component Agencies.

The contractor shall coordinate (e.g., configure) with the Government to provide VoIP services to DHS Component Agencies.

C.5.2.2.4.2 AUDIO VISUAL (AV) AND VIDEO TELECONFERENCING (VTC)

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Audio Visual (AV) and Video Teleconferencing (VTC) infrastructure.

The St. Elizabeths Campus will include approximately 500 spaces (e.g., facilities, conference rooms, multi-media rooms, team rooms) requiring AV and VTC infrastructure.

AV and VTC infrastructure includes:

a. Video Display Walls
b. Knowledge Walls

c. VTC Suites
d. Room Management and Reservation Services
e. AV and VTC Management and Control Services
f. AV Matrix Recorders
g. Bridging Services to St. Elizabeths Campus Signage (e.g., Internet Protocol Television (IPTV))
h. Bridging Services for Conference Calls and VTCs

St. Elizabeths Campus facilities requiring extensive AV and VTC infrastructure includes:

a. Campus Media Center
b. Hitchcock Hall Auditorium and Conference Center
c. Press Center

The contractor shall coordinate (e.g., configure) with the Government to provide AV and VTC services to DHS Component Agencies.

C.5.2.2.4.3 INTERNET PROTOCOL (IP) TELEVISION (IPTV) SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IPTV Services back-end systems.

The St. Elizabeths Campus IPTV services back-end systems integrate and interoperate with the St. Elizabeths Campus IT infrastructure, and provide subscriber management, 16 High Definition (HD) television channels, four digital signage channels, two internal live/rebroadcast channels, and internal Video On Demand (VOD) services to AV and VTC services, digital signage, and end-point devices.

The IPTV services back-end systems are expandable to support 400 channels of High Definition (HD) and IP video (e.g., streaming). Input sources include St. Elizabeths Campus data feeds (e.g., Campus Media Center, Hitchcock Hall Auditorium and Conference Center, Press Center), cable, satellite, broadcast, and VOD.

C.5.2.2.4.4 ENTERPRISE MANAGEMENT SERVICES (EMS)

The contractor shall perform requirements analysis and design to develop, expand, and extend the IT Services Management Suite also referred to as the St. Elizabeths Campus Enterprise Management Services (EMS) back-end systems.

There shall be independent EMS back-end systems for each classification level (i.e., UNCLASSIFIED, SECRET, and TOP SECRET (TS)).

The EMS back-end systems shall integrate the management of the St. Elizabeths Campus IT infrastructure, for each classification level, allowing contractor personnel, Government personnel, and other Government contractors to manage and monitor the St. Elizabeths Campus IT infrastructure.

The contractor shall coordinate (e.g., configure) with the DHS Component Agencies to provide integration with DHS Component Agencies Service Desk Enterprise Management Suites.

C.5.2.3 SUBTASK 3 – PHYSICAL SECURITY

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus physical security services.

The physical security services integrate and interoperate with the St. Elizabeths Campus IT infrastructure (i.e., SBUCAN, Physical Security Network, and Ethernet) using the following:

a. Access Controls:
   i. Access Cards - HSPD-12
   ii. Card Readers - Systems
   iii. Card Readers - Proximity
   iv. Card Readers - Hand Held
   v. Card Readers - PIN and/or Biometric
   vi. Card Readers - Turnstiles
   vii. Access Control Systems - Secure Spaces
   viii. Access Control Systems - Enterprise
   ix. Visitor Management Services

b. Life-Safety:
   i. Emergency Call Stations
   ii. Crash lighting system with local and central control system
   iii. Guard Crash Alarm and Intercom Services
   iv. LMR Services
   v. Life-Safety Duress Systems
   vi. Notification System - Multi-Media Emergency
   vii. Notification System - Public

c. Perimeter:
   i. Fence Sensor Systems
   ii. Barrier Control Systems - Hydraulic
   iii. Barrier Control Systems - Electric
   iv. Barrier Control Systems - Bollards
   v. Barrier Control Systems - Plate
   vi. Intrusion Detection Systems - Ported Coax Sensors
   vii. Microwave Motion Sensors - Mono-static
   viii. Microwave Motion Sensors - B-static
   ix. Magnetometers (Fixed and Portable)
   x. Perimeter Map Display Systems
   xi. Under Vehicle Surveillance Systems (UVSS) and Under Vehicle Inspection Systems (UVIS)
   xii. X-Ray - Package (Belt Driven)
   xiii. X-Ray - Pallet

   xiv. X-Ray - Truck

d. Video Monitoring:

   i. Cameras - Analog
   ii. Cameras - Digital
   iii. Cameras - Environmental Day/Night Tube
   iv. Cameras - Mega-Pixel
   v. Cameras - Outdoor True Day/Night Dome
   vi. Cameras - Thermal Imaging
   vii. Lighting - Light Emitting Diode (LED)
   viii. Lighting - Motion Activated
   ix. Lighting - Infrared LED (IFR LED)
   x. Video Switches - Analog
   xi. Video Switches - Digital
   xii. Video - Analytics
   xiii. Video - Surveillance
   xiv. Video - Recording System
   xv. Video - Recording Retention System

e. Monitoring

   i. Detection Systems – Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE), Personnel
   ii. Detection Systems - CBRNE, Vehicle
   iii. Detection Systems - Radiation
   iv. Detection Systems - Chemical
   v. Identification Systems - Isotope

f. Physical Intrusion Detection Systems

   i. Motion Sensors for secure spaces
   ii. Motion Sensors for non-secure spaces
   iii. Door Position Switches for secure spaces
   iv. Door Position Switches for non-secure spaces

C.5.2.3.1 ACCESS CONTROL SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus access control services.

The access control services shall comply with The Risk Management Process for Federal Facilities Interagency Security Committee (ISC) standards and Intelligence Community Directive (ICD) 705 requirements, and be integrated and interoperable with the St. Elizabeths Campus IT infrastructure, HSPD-12 identification cards (i.e., DHS PIV cards, DoD Common Access Cards (CACs)), and GSA PBS-issued construction badges (e.g., MiFare cards).

The access control services shall at a minimum provide the following:

a. Access control services for St. Elizabeths Campus and facilities in compliance with ISC standards.
b. Access control services for SCIFs or other high security areas in compliance with ISC standards and ICD 705 requirements and Underwriters Laboratory (UL) standards.
c. Visitor Management Services in compliance with ISC standards.

The contractor shall coordinate with GSA PBS for the interoperability and compatibility of GSA PBS construction badges with Access Control Services.

C.5.2.3.2 LIFE-SAFETY SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus Life-Safety Services.

C.5.2.3.2.1 MULTI-MEDIA EMERGENCY NOTIFICATION SERVICES AND PUBLIC NOTIFICATION SERVICES

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus Multi-Media Emergency Notification Services (ENS) and Public Notification Services (PNS). The ENS and PNS services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure and shall provide audio, visual, and data-based notifications to the St. Elizabeths Campus.

The ENS and PNS services design shall at a minimum provide notifications by the following means:

a. Public Address (PA) system
b. E-mail
c. Text Messages
d. IPTV Services
e. Digital Signage
f. VoIP Services
g. Cellular Telephones
h. Emergency Call Stations
i. LMR

The contractor shall coordinate (e.g., integrate and configure) with GSA PBS and Potomac Services Center (PSC) to ingrate the ENS and PNS services with the St. Elizabeths Campus fire alarm and emergency communication services.

The contractor shall coordinate (e.g., integrate and configure) with DHS, Federal, state, and local municipalities to provide ENS and PNS services on the St. Elizabeths Campus.

C.5.2.3.2.2 EXTERNAL LIFE-SAFETY COMMUNICATIONS

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus external life-safety communication services.

The external life-safety communication services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure and shall, at a minimum, provide two-way communications (e.g., data, voice, and video) with the following:

a. St. Elizabeths Campus Security Operations Center (CSOC)
b. St. Elizabeths Campus Guard Stations
c. Washington, D.C. First Responders
d. Washington, D.C. Command Center
e. DHS FPS
f. GSA PBS
g. GSA PSC
h. DHS Office of the Chief Security Officer (OCSO)

The contractor shall coordinate with the Government to provide external life-safety communication services to the St. Elizabeths Campus.

C.5.2.3.2.3 EMERGENCY CALL STATIONS (ECS)

The contractor shall perform requirements analysis and design for the St. Elizabeths Campus Emergency Call Station (ECS) services. The contractor shall install ECS in parking garages, outdoors, indoors, and in tunnels.

The ECS services design shall provide ECS with the following capabilities:

a. Compliance with Americans with Disabilities Act (ADA) and Section 508.
b. Establish emergency audio and video two-way communications between the ECS and St. Elizabeths Campus life-safety.
c. Establish communications between the ECS and St. Elizabeths Campus life-safety via hands free, one button operations (e.g., emergency button).
d. Report the location of activated ECS on the St. Elizabeths Campus.
e. Identify the activation of an ECS on the St. Elizabeths Campus by visual means (e.g., strobe light).
f. Identify the activation of an ECS on the St. Elizabeths Campus by audible means (e.g., alarm, siren).
g. Annunciation of St. Elizabeths Campus ENS and PNS services information.
h. Display St. Elizabeths Campus ENS and PNS services information.
i. Conduct surveillance using Closed Circuit Television (CCTV).
j. Multiple mounting and anchoring options (e.g., self-standing, poles, and walls).
k. Powered via Power Over Ethernet (POE) technologies.

C.5.2.3.3 PERIMETER SECURITY SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus perimeter security services.

C.5.2.3.3.1 VIDEO SURVEILLANCE SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus video surveillance services.

The St. Elizabeths Campus will include the capability to integrate approximately 5,000 plus security cameras. The security cameras are located at St. Elizabeths Campus security gates, building and facility interiors and exteriors, building and facility entrance and exit points, SCIF entrance and exit points, perimeter fencing, and other locations identified by the Government.

The St. Elizabeths Campus security cameras are augmented with lighting, motion detectors, and Infrared Light Emitting Diodes (IFR LED).

The video surveillance services design shall integrate and be interoperable with the St. Elizabeths Campus IT infrastructure.

The video surveillance services design shall at a minimum provide the following:

a. Video surveillance camera coverage areas.
b. Video surveillance types and placements.
c. Video surveillance lighting coverage areas.
d. Video surveillance lighting types and placements.
e. Motion detector coverage areas.
f. Motion detector types and placements.
g. Motion detector alarm reporting.
h. Motion detector location reporting.
i. Video surveillance recording and retention.
j. Video surveillance playback

C.5.2.3.3.2 PHYSICAL INTRUSION DETECTION SERVICES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus physical intrusion detection services.

At a minimum, the physical intrusion detection services design shall provide the following:

a. Motion sensors for secure and non-secure building and facilities.
b. Door position switches and sensors for secure and non-secure building and facilities.

C.5.2.4 SUBTASK 4 - SPECIAL FACILITIES

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure in special facilities.

Special facilities have been identified by the Government as providing critical services to DHS, the St. Elizabeths Campus IT infrastructure, St. Elizabeths Campus life-safety, or require special Government considerations.

C.5.2.4.1 NON-DHS COMPONENT AGENCIES AND COMMERCIAL VENDORS

The contractor shall perform requirements analysis and design to develop, expand, and extend the St. Elizabeths Campus IT infrastructure to and within Non-DHS Component Agencies and commercial vendor facilities on the St. Elizabeths Campus.

Non-DHS Component Agencies are other Government Agencies (e.g., GSA) that occupy facilities on the St. Elizabeths Campus and require St. Elizabeths Campus IT infrastructure services (e.g., VoIP and connectivity).

Commercial vendors are non-Government entities (e.g., food services, credit union, dry cleaners, fitness center, child care centers, and barber), that are sponsored by DHS Component Agencies and Non-DHS Component Agencies that occupy facilities on the St. Elizabeths Campus and require St. Elizabeths Campus IT infrastructure services (e.g., VoIP and connectivity).

C.5.2.5 SUBTASK 5 - SYSTEM ENGINEERING LIFE CYCLE (SELC) DELIVERABLES

The contractor shall develop and deliver System Engineering Life Cycle (SELC) packages (e.g., documents, artifacts) in accordance with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, industry, and Government best practices to support the development, expansion, and extension of the St. Elizabeths Campus.

C.5.2.5.1 SYSTEM DEFINITION REVIEWS

The contractor shall develop and deliver **System Definition Review (SDR) Packages** (Section F, Deliverable 20) in accordance with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, Appendix B: SELC Artifact Matrix.

C.5.2.5.2 PRELIMINARY DESIGN REVIEWS (PDR)

The contractor shall develop and deliver **Preliminary Design Review (PDR) Packages** (Section F, Deliverable 21) in accordance with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, Appendix B: SELC Artifact Matrix.

C.5.2.5.3 CRITICAL DESIGN REVIEWS (CDR)

The contractor shall develop and deliver **Critical Design Review (CDR) Packages** (Section F, Deliverable 22) in accordance with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, Appendix B: SELC Artifact Matrix.

As applicable, the contractor shall develop and deliver **Integration Readiness Review (IRR) Artifacts** (Section F, Deliverable 23) in accordance with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, Appendix B: SELC Artifact Matrix, as part of CDR Packages.

The contractor shall develop and deliver **Engineering Implementation Plans (EIPs)** (Section F, Deliverable 24) as part of CDR Packages.

C.5.2.6 SUBTASK 6 - TRANSITION AND TRANSFER TO IMPLEMENT, SECURE, AND TEST

On Government approval of CDR packages, Task 2 Requirements Analysis and Design is formally complete.

The contractor shall transition and transfer CDR packages to Task 3 - Implement, Test, and Secure Services after CDR approval.

C.5.3 TASK 3 - IMPLEMENT, TEST, AND SECURE SERVICES

The contractor shall use a systems engineering methodology to implement, test, and secure the St. Elizabeths Campus IT infrastructure that includes the implementation, operational testing, configuring, accrediting, and transitioning to O&M in compliance with Government architectures, standards, design guides, and policies.

The contractor shall implement, test, and secure the St. Elizabeths Campus IT infrastructure in accordance with approved Government designs.

The contractor shall not deviate, substitute, or otherwise modify Government-approved designs without prior Government approval.

The contractor, on identification of any deviations, substitutions, or other modifications to Government-approved designs, shall immediately stop all implement, test, and secure activities of the design and report it to the Government. The Government will provide instructions to the contractor on how to proceed with implement, test, and secure when deviations, substitutions, or other modifications are reported to the Government.

C.5.3.1 SUBTASK 1 - IMPLEMENT, TEST, AND SECURE MANAGEMENT

The contractor shall comply and execute in accordance with the DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, the DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, and other industry and Government systems engineering best practices (e.g., PMBOK, ITIL, and PRINCE2).

The Government will assign “project” status to implement, test, and secure activities for the St. Elizabeths Campus IT infrastructure based on technical (e.g., system boundaries and security boundaries), operational, or organizational demarcations. The Government will organize projects into an overarching St. Elizabeths Campus IT infrastructure portfolio.

The contractor in support of the St. Elizabeths Campus IT infrastructure portfolio, for each project shall:

a. Develop and manage to project plans.
b. Develop and manage to project WBS.
c. Develop and manage to project schedules.
d. Develop and manage to costs.
e. Identify and manage to risks and issues.
f. Identify, coordinate, and manage implement, test, and secure activities with contractor personnel, Government personnel, and other Government contractors.

g. Identify, coordinate, and manage communications (e.g., technical, schedules, risks) with contractor personnel, Government personnel, and other Government contractors.
h. Identify, coordinate, and manage the reporting of project status with contractor personnel, Government personnel, and other Government contractors.
i. Identify, coordinate, and manage the reporting of testing status with contractor personnel, Government personnel, and other Government contractors.
j. Identify, coordinate, and manage the transitioning of IT infrastructure to O&M services.
k. Identify, coordinate, and manage the transfer of artifacts and Configuration Items (CIs) (e.g., drawings, licenses) to O&M services.
l. Identify and report any deviations, substitutions, or other modifications to Government-approved designs to the Government.

The contractor shall develop a St. Elizabeths Campus **IT Infrastructure Implement, Test, Secure Master Plan** (Section F, Deliverable 25). The St. Elizabeths Campus IT Infrastructure Implement, Test, Secure Master Plan shall identify and describe how the contractor shall comply with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, DHS 4300A Sensitive Systems Handbook, DHS 4300B National Security Systems Policy Directive, and other industry and Government systems engineering best practices.

C.5.3.2 SUBTASK 2 - IMPLEMENT

C.5.3.2.1 IMPLEMENT

The contractor shall implement the St. Elizabeths Campus IT infrastructure in accordance with approved Government designs (i.e., TOR Task 2 - Requirements Analysis and Design).

C.5.3.2.2 CAMPUS AND BUILDING OUTSIDE PLANT WIRING

The contractor shall install FOC and copper cables in GSA PBS-provided utility tunnels and direct buried cable ducts (e.g., conduit).

C.5.3.2.3 CAMPUS AND BUILDING INSIDE PLANT WIRING

The contractor shall install FOC and copper cables in GSA PBS-provided pathways for vertical fiber, horizontal fiber and copper, and ladder racks for building and facilities IT infrastructure.

C.5.3.2.4 PROOF OF CONCEPTS

The contractor shall implement proof-of-concept designs to support technical, performance, integration, and interoperability evaluations of technologies and solutions.

C.5.3.3 SUBTASK 3 - TEST

The contractor shall conduct testing in accordance with Government-approved test plans to verify and validate the proper installation, operations, and performance of St. Elizabeths Campus IT infrastructure.

C.5.3.3.1 IMPLEMENTATION TESTING

The contractor shall conduct implementation testing in accordance with Government-approved test plans.

C.5.3.3.2 ACCEPTANCE TESTING

The contractor shall conduct acceptance testing in accordance with Government-approved CDR packages (i.e., IRR artifacts) and participate in ORRs.

The contractor shall develop an **Acceptance Testing Report** (Section F, Deliverable 26), which documents the type of tests conducted, the raw test data, the testing results (e.g., pass, fail), and a narrative analysis of the testing results (e.g., explanation of failures, deficiencies, and risks).

C.5.3.4 SUBTASK 4 - SECURE

The contractor shall securely anchor and mount St. Elizabeths Campus IT infrastructure in appropriate enclosures (e.g., racks, cabinets, cable trays, and risers).

The contractor shall securely configure St. Elizabeths Campus IT infrastructure in accordance with Government policies, guidelines, and mandates.

C.5.3.5 SUBTASK 5 - TRANSITION AND TRANSFER TO O&M

The contractor shall develop a **Transition and Transfer to O&M Checklist** (Section F, Deliverable 27) which identifies all of the St. Elizabeths Campus IT infrastructure to be transitioned to Task 4 O&M Services and all artifacts and CIs that are to be transferred to Task 4 O&M Services on completion of Task 3 - Implement, Test, and Secure Services projects. The Transition and Transfer to O&M Checklist shall identify the transition and transfer dates for IT infrastructure, artifacts, and CIs.

The contractor (e.g., O&M Lead) shall review, verify, and sign Transition and Transfer to O&M Checklists.

The contractor shall obtain Government signature on Transition and Transfer to O&M Checklists. On Government signature, Task 3 – Implement, Test, and Secure Services project is complete.

C.5.4 TASK 4 - OPERATIONS AND MAINTENANCE (O&M) SERVICES

The contractor shall perform all O&M services necessary to operate, manage, maintain, and secure the current St. Elizabeths Campus IT infrastructure and IT infrastructure that will be transitioned to O&M. The St. Elizabeths Campus IT infrastructure is described in the CONOPS.

The contractor shall develop, implement, and maintain a comprehensive **IT Service Management Plan** (Section F, Deliverable 28) that documents the contractor's organizational structure, processes, procedures, tools, standards, and governing policies for delivering O&M services for St. Elizabeths Campus IT infrastructure. The IT Service Management Plan identifies where IT artifacts are stored (e.g., systems files). The IT Service Management Plan shall include at a minimum:

a. Organizational chart.
b. Functional team descriptions.

c. Lines of authority.
d. Communication plans.
e. Staffing methodology.
f. Staffing matrix with skillset breakdown.
g. Quality control methodology.
h. Risk management methodology.
i. Service Level Management (SLM) methodology.
j. Knowledge management methodology.
k. Account administration methodology.
l. Internal dependencies.
m. External dependencies.

C.5.4.1 SUBTASK 1 – IT SERVICE DESK

The contractor shall operate and maintain a Tier 1, Tier 2, and Tier 3 level IT Service Desk to support the St. Elizabeths Campus IT infrastructure.

The contractor shall operate the Tier 1, Tier 2, and Tier 3 Service Desk Monday through Friday during the core hours of 6:00 a.m. to 6:00 p.m. Eastern Time (ET).

Historic St. Elizabeths Campus IT Service Desk data (i.e., requests, incidents, work orders) is provided in the St. Elizabeths Campus IT Service Desk Data 2016 06 06 to 2017 06 05 attachment (Section J, Attachment Tech-O).

The contractor-operated IT Service Desk shall execute incident management and request fulfillment in accordance with industry and Government best practices (e.g., ITIL). Incident management and request fulfillment encompasses receipt and notification, categorization, prioritization, resolution/fulfillment in accordance with incident and request models, and closure. Service requests requiring design and engineering support shall be handled using a separate request model.

The contractor, via the IT Service Desk, shall execute incident management and request fulfillment to meet SLAs and performance standards.

The contractor, via the IT Service Desk, shall refine and implement IT Service Desk workflows (e.g., decision trees and scripts) aligned to incident and request models to ensure accurate and complete information is consistently requested, received, and documented to support incident management and request fulfillment. Incident management and request models shall be maintained in the campus knowledge management system.

The contractor-operated IT Service Desk shall communicate, coordinate, and collaborate with contractor personnel, Government personnel, and other Government contractors in the execution of incident management and request fulfillment.

The contractor-operated IT Service Desk shall facilitate the exchange (e.g., integration and interfaces) of incident information with other DHS Component Agency IT Service Desks in the execution of incident management and request fulfillment.

The contractor shall configure and program the Service Desk Enterprise Management Suite to provide required data points and reports, which shall include capture of related configuration items for tickets and appropriate setting of ticket status needed for SLAs performance calculation.

The contractor shall prepare an **Incident Management Model** (Section F, Deliverable 30), which identifies common types of incidents and the process for handling each incident type (e.g., who, what, when, and how) in a pre-defined manner, any required notifications and precautions, and escalation procedures. Processes for determining status, categorizing, prioritization, and SLA assignment shall also be included in the Incident Management Model.

The contractor shall prepare a **Request Fulfillment Model** (Section F, Deliverable 31), which identifies types of service requests and the process for handling each type (e.g., who, what, when, and how) in a pre-defined manner, workflows for approvals and pre-requisite requirements, any required notifications, and escalation procedures. Processes for determining status, categorizing, prioritization, and SLA assignment shall also be included in the Request Fulfillment Model.

The contractor shall prepare a **Ticket Analysis Report** after assuming full IT Service Desk responsibility (Section F, Deliverable 32), which provides an analysis of tickets by prioritization and by root cause. The Ticket Analysis Report shall include a ticket analysis summary including recommendations for future actions and risk mitigations.

C.5.4.1.1 IT SERVICE DESK - TIER 1

The contractor shall provide IT Service Desk - Tier 1 services for the St. Elizabeths Campus IT infrastructure. The IT Service Desk - Tier 1 shall serve as the initial point of entry for requests, incidents, and work orders for the St. Elizabeths Campus IT infrastructure. Tier 1 services are responsible for capturing all pertinent information required to resolve requests, incidents, and work orders and appropriately triaging and prioritizing tickets. Tier 1 services are responsible for resolving basic and standard requests, incidents, and work orders.

C.5.4.1.2 IT SERVICE DESK -TIER 2

The contractor shall provide IT Service Desk - Tier 2 services for the St. Elizabeths Campus. The Tier 2 Service Desk shall resolve requests, incidents, and work orders for the St. Elizabeths Campus IT infrastructure that cannot be processed or resolved by the Tier 1 Service Desk.

C.5.4.1.3 IT SERVICE DESK - TIER 3

The contractor shall provide IT Service Desk - Tier 3 services for the St. Elizabeths Campus. The Tier 3 Service Desk shall resolve requests, incidents, and work orders for the St. Elizabeths Campus IT infrastructure that cannot be processed or resolved by either the Tier 1 or Tier 2 Service Desk.

The contractor’s Tier 3 services shall provide the highest level of technical and professional troubleshooting services for the St. Elizabeths Campus IT infrastructure. The Tier 3 services shall be responsible for the elevation of all requests, incidents, and work orders that cannot be resolved by the Tier 3 Service Desk to commercial system and service providers for assistance and resolution.

C.5.4.2 SUBTASK 2 – OPERATIONS CONTROL

The contractor shall provide operations control services that includes two core activities: network monitoring and security monitoring. The specific operational activities are described in the CONOPS. Information regarding the reporting of security events is specified in DHS 4300A Sensitive Systems Handbook and DHS 4300B National Security Systems Policy Directive. Under this Subtask, the contractor shall provide monitoring services for the St. Elizabeths IT infrastructure 24x7x365. The unclassified IT infrastructure (i.e., SBUCAN) shall be monitored from the IT Operations Center (ITOC). The classified IT infrastructure (i.e., SCAN and TSCAN) shall be monitored from the campus Enterprise Operations Center (EOC). The ITOC and EOC are located on St. Elizabeths Campus.

The contractor shall prepare an **Initial After Action Report** (Section F, Deliverable 33) and a **Final After Action Report** (Section F, Deliverable 34) for all incidents that result in a service disruption or outage. The After Action Reports shall include submission date, author, event description, applicable ticket numbers, date of occurrence, duration and chronology of events, services and systems affected, customers affected, troubleshooting steps and analysis; and resolution and corrective action, root cause analysis, preventative actions/action items, lessons learned, knowledge base updates, and reviewers.

C.5.4.2.1 CAMPUS NETWORK OPERATIONS CENTER (NOC)

The contractor shall manage and monitor the St. Elizabeths Campus Network Operations Center (NOC). The St. Elizabeths Campus NOC monitors and manages the St. Elizabeths Campus IT infrastructure to ensure CIA of the IT infrastructure to include WAN connectivity (e.g., demarcation points). The St. Elizabeths Campus NOC operates as a "DHS Component Network Operations Center."

The contractor shall operate the St. Elizabeths Campus NOC 24x7x365. Specifically, the St. Elizabeths Campus NOC supports Tier 2 and Tier 3 Service Desk for critical, high, medium, and low incidents for the St. Elizabeths Campus IT infrastructure during core hours Monday through Friday of 6:00 a.m. to 6:00 p.m. Eastern Time. The St. Elizabeths Campus NOC provides Tier 2 and Tier 3 Service Desk services for critical incidents outside of core hours.

The contractor shall monitor automated alerts and respond accordingly to resolve alerts. As required, the contractor shall coordinate with Government and designated non-Government personnel if an alert cannot be resolved based on severity of the alert. The contractor shall ensure that potential points of failures within the IT infrastructure are appropriately monitored via automated alerts to provide adequate advance notice of problems to enable proactive resolution before services are degraded and/or disrupted.

The contractor shall escalate all incidents causing service disruption to the Government and others identified in the communications plan as identified in the CONOPS.

C.5.4.2.2 CAMPUS SECURITY IT OPERATIONS CENTER (IT SOC)

The contractor shall manage and monitor the St. Elizabeths Campus Security IT Operations Center (IT SOC).

The St. Elizabeths Campus IT SOC monitors and manages the St. Elizabeths Campus IT infrastructure to ensure CIA, Information Assurance (IA), and cyber security of the IT infrastructure. The St. Elizabeths Campus IT SOC operates as a "DHS Component Security Operations Center."

The contractor shall operate the St. Elizabeths Campus IT SOC 24x7x365. Specifically, the St. Elizabeths Campus IT SOC supports the Tier 2 and Tier 3 Service Desk for critical, high, medium, and low incidents for the St. Elizabeths Campus IT infrastructure during core hours Monday through Friday of 6:00 a.m. to 6:00 p.m. Eastern Time. The St. Elizabeths Campus IT SOC provides Tier 2 and Tier 3 Service Desk services for critical incidents outside of core hours.

The contractor shall monitor all St. Elizabeths Campus IT infrastructure security components, including Intrusion Detection Systems (IDSs) and Policy Enforcement Points (PEPs). The contractor shall perform the following:

a. Monitor IT infrastructure for intrusion activity, take appropriate steps to mitigate any suspected intrusion, and maintain the availability of the IT infrastructure to authorized users.
b. Perform incident response per DHS 4300A Sensitive Systems Handbook Attachment F Incident Response (Section J, Attachment Tech-P). Perform computer forensics, law enforcement evidence collection, and preservation efforts in support of IT infrastructure.
c. Perform assessments quarterly (or as directed) at all major nodes, such as gateways where data is stored, and report the results of such findings to the Government.

Perform security and anti-virus scans of the IT infrastructure in accordance with Government procedures. The contractor shall use automated delivery capabilities to the maximum extent possible to push security and anti-virus software signature updates to the IT infrastructure. The contractor shall report all IT infrastructure components not in compliance with security requirements to the Government.

C.5.4.2.3 CAMPUS SECURITY OPERATIONS CENTER (C-SOC)

St. Elizabeths Campus Security Operations Center (C-SOC) is managed and operated by Government personnel to monitor the St. Elizabeths Campus physical security (e.g., 5,000 surveillance cameras), access controls (e.g., perimeter, facilities), and life-safety services.

The contractor shall provide O&M support for the IT infrastructure supporting the St. Elizabeths C-SOC and Physical Security Equipment Room.

The contractor shall perform the following:

a. Monitor physical security services, access control services, and life-safety services for 24x7x365 for operations and availability.
b. Perform incident response to physical security services, access control services, and life-safety services degradations or disruptions to ensure the 24x7x365 security of the St. Elizabeths Campus and facilities.

C.5.4.3 SUBTASK 3 – OPERATIONS MANAGEMENT

The contractor shall provide operations management for the St. Elizabeths Campus IT infrastructure and perform support activities described in the CONOPS.

The contractor shall prepare and deliver an **O&M Status Report** (Section F, Deliverable 35), that identifies:

a. SLA analytics by week, quarter, six months, and year.
b. IT infrastructure degradations or outages.
c. IT Service Desk analytics for incidents, requests, and work orders (e.g., open, closed, and pending).
d. IT Service Desk incidents, requests, and work orders in violation of SLAs.
e. IT Service Desk incidents, requests, and work orders requiring Government direction or assistance.
f. Operations Management Summary of completed activities and planned activities for the next reporting period.
g. IT Security Management Summary of completed activities and planned activities for the next reporting period.
h. Technical Management Summary of completed activities and planned activities for the next reporting period.
i. List of Deliverables furnished to the Government.
j. Schedule of Deliverables with planned delivery dates to the Government.

C.5.4.3.1 IT INFRASTRUCTURE MANAGEMENT

The contractor shall manage and maintain the St. Elizabeths Campus IT infrastructure to ensure CIA of the IT infrastructure to include WAN connectivity (e.g., demarcation points).

The contractor shall perform the following IT infrastructure management services:

a. Manage and maintain the operational performance of the IT infrastructure.
b. Manage and maintain the allocations and capacities of the IT infrastructure:
    i. Manage and maintain Load Balancing of the IT infrastructure.
    ii. Manage and maintain the IP Addressing.
    iii. Manage and maintain Media Access Control (MAC) Addresses.
    iv. Manage and maintain Virtual Local Area Networks (VLANs).
c. Manage and maintain Quality Control (QC) of the IT infrastructure.
d. Manage and maintain operational performance risks to the IT infrastructure.
e. Manage and maintain monitoring tools, probes, and agents of the IT infrastructure.
f. Manage the escalation and prioritization of incidents, requests, and work orders.
g. Manage the life cycle of the IT infrastructure:
    i. Manage configurations and parameters.
    ii. Manage installation of patches, updates, service packs, and upgrades.
    iii. Manage recapitalization.
    iv. Manage life cycle replacement.
h. Manage the process of transitioning IT infrastructure from implementation to O&M.
i. Manage commercial vendor relationships required to support IT infrastructure.
j. Identify process and performance efficiencies and improvements.

k. Manage communications with contractor personnel, Government personnel, and other Government contractors for:
   i. IT infrastructure changes.
   ii. Planned and unplanned service disruptions.

Historically, there have been two monthly standard patch windows for the installation of patches, updates, service packs, and upgrades; typically, these are conducted the second and third weekend of each month. Additional patch windows may occur outside of the standard patch windows for other reasons (e.g., emergency security patches).

The contractor shall prepare a monthly **IT Infrastructure Utilization Monthly Report** (Section F, Deliverable 36) that includes average and maximum utilization during the month (daily data), with annotations of performance anomalies.

The contractor shall prepare a quarterly **IT Infrastructure Utilization Quarterly Report** (Section F, Deliverable 37) that provides a roll-up summary of the monthly IT Infrastructure Utilization Report and, in addition, includes average and maximum utilization of the back-end service delivery systems during the quarter with annotations of performance anomalies. The purpose of the IT Infrastructure Utilization Quarterly Report is to provide an early warning of systems that are nearing their performance capacity.

C.5.4.3.1.1 PHYSICAL SECURITY IT INFRASTRUCTURE MANAGEMENT

The contractor shall manage the St. Elizabeths physical security SBUCAN IT infrastructure to ensure CIA.

The contractor shall perform the following physical security SBUCAN IT infrastructure management services:

a. Manage and maintain physical security of endpoint devices (e.g., cameras, turnstiles, and x-ray machines).
b. Manage and maintain physical security of servers, workstations, desktops, and laptops.
c. Manage and maintain physical security of back-end systems (e.g., video monitoring and recording services and storage).
d. Manage and maintain physical security of virtual IT infrastructure (e.g., servers and virtual desktops).
e. Manage and maintain physical security of Ethernet infrastructure.
f. Manage and maintain physical security of preventative maintenance (e.g., plan, schedule, and report).

C.5.4.3.2 ASSET MANAGEMENT

The contractor shall perform asset management inclusive of life cycle management of the St. Elizabeths Campus IT infrastructure in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual (Section J, Attachment Tech-Q) and DHS Directives Systems Directive Number 119-03 Personal Property Management Program (Section J, Attachment Tech-R). Asset management includes the management of IT assets (e.g., hardware and software) and spares from initial installation and the asset's operational lifetime to final disposition and disposal.

The contractor shall perform the following asset management services:

a. Manage and secure IT assets (e.g., materials, tools, and spares).
b. Process IT assets in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual and DHS Directives Systems Directive Number 119-03 Personal Property Management Program.
c. Maintain IT asset records in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, Section 2.6**.**
d. Report IT assets in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, Section 2.6.
e. Conduct IT asset monitoring and inventories of all IT assets in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, Section 2.7.
f. Process IT assets to ensure that they are properly security-level identified, tagged, and recorded in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, Section 4.5.
g. Process and record personal property in accordance with DHS Manual 119-03-001-01 Personal Property Asset Management Program Manual, Section 4.6.
h. Identify, correlate, manage, and maintain IT assets status (e.g., ordered, received, processed, configured, deployed, reserved, and disposed).
i. Identify, correlate, manage, and maintain IT assets physical locations (e.g., building and room).
j. Identify, correlate, manage, and maintain IT asset associated warranty and service support agreements (e.g., contracts and Enterprise License Agreements (ELAs)) for IT assets.
k. Identify, correlate, manage, and maintain software license accountability, allocation, assignment, and installation.
l. Process and return uninstalled IT assets to available surplus inventory.
m. Process, manage, track, and report “return to manufacture requests” (e.g., Return Merchandise Authorization (RMA)) for IT assets requiring service.
n. Identify, correlate, manage, and maintain IT assets with CIs.
o. Manage and maintain the asset management services database schema and rules for data standardization and normalization.
p. Develop and coordinate for Government approval of purchase requests for new IT assets.

The contractor shall configure, develop, and maintain the Government Asset Management Services (e.g., system) to provide the following capabilities:

a. Support the recording, updating, and managing of Accountable and Non-Accountable IT assets (hardware and software assets).
b. Support interfaces and integration with Configuration Management Database (CMDB) Services.
c. Support interfaces and integration with Change Management Services.
d. Support interfaces and integration with Release Management Services.

e. Support interfaces and integration with IT Service Desk Services.
f. Support interfaces and integration with automated IT infrastructure discovery services.
g. Support interfaces and integration with Other Government Services (e.g., Sunflower).
h. Support and maintain IT asset queries and reporting capabilities by Asset Management Database elements (e.g., data fields).
i. Support and maintain master data management (e.g., format and structure).

The contractor shall manage and maintain an **Asset Management Database** that is compatible with Government services and supports asset management services.

The contractor shall manage and maintain an Asset Management Database Schema (e.g., Entity Relationship Diagram (ERT)) and associated Asset Management Database Data Dictionary.

The contractor shall deliver an updated **Asset Management Database Schema** (Section F, Deliverable 38) and **Asset Management Database Data Dictionary** (Section F, Deliverable 39) identifying changes, additions, and deletions.

The contractor shall prepare an **Asset Management Inventory Report** (Section F, Deliverable 40) that provides the data contained within the Asset Management Database. The Asset Management Inventory Report shall identify the following:

a. The date the data was collected from the Asset Management Database.
b. Unreconciled IT assets.
c. IT asset data fields that do not conform to the data dictionary (i.e., Master Data Management).
d. IT assets that are within six months of End of Life (EOL).
e. Replacement options for identified EOL IT assets.
f. IT assets that are within six months of manufacturer warranty expiration.
g. IT assets that are within six months of service contract expiration.

The contractor shall provide the Asset Management Inventory Report in Excel, .pdf, and Comma Separated Value (CSV) file formats. The Asset Management Inventory Report Excel file shall be filterable by column by listed data fields identified in the Asset Management Database Schema and corresponding data dictionary.

The contractor shall comply with DHS Manual 119-03-001-01, 2017-001 PP Bulletin Consolidated Asset Portfolio and Sustainability Information System (CAPSIS) Monthly Reporting Requirements (Section J, Attachment Tech-S).

The contractor shall deliver the **CAPSIS Monthly Report** (Section F, Deliverable 79). A SAMS Data Upload Template is provided as a TOR attachment (Section J, Attachment Tech-W).

C.5.4.3.2.1 ASSET DISPOSAL

The contractor, upon identification or notification of St. Elizabeths Campus IT infrastructure decommissioning, shall perform the following decommission and disposal services:

a. Identify IT infrastructure that can be reused or reissued (e.g., software licenses).
b. Update the asset management services (e.g., disposed).
c. Update Enterprise License Agreements (ELAs) as required.

d. Update service support agreements as required.
e. Complete and submit to the Government all required documentation for decommissioning.
f. Prepare IT infrastructure for Government surplus, donation, recycling, or disposal as required.
g. Destroy or sanitize (e.g., degauss hard drives) IT infrastructure utilizing approved methods and procedures as required.
h. Coordinate and manage the transportation of decommissioned IT infrastructure to disposal destination (e.g., surplus facility, recycling center, and waste management facilities).

The contractor shall sanitize St. Elizabeths Campus IT infrastructure storage devices in accordance with National Security Agency/Central Security Service (NSA/CSS) Policy Manual 9-12 (Section J, Attachment Tech-T) prior to recycling or disposal.

The contractor shall prepare an **IT Infrastructure Disposal Report** (Section F, Deliverable 62) that identifies the St. Elizabeths Campus IT infrastructure that was decommissioned since the last Government-accepted IT Infrastructure Disposal Report.

C.5.4.3.2.2 SPARES MANAGEMENT

The contractor shall prepare a **Spares Methodology and Spares List** (Section F, Deliverable 41) that describes the contractor’s methodology for determining sparing levels and spare quantities. The Spares Methodology and Spares List shall contain:

a. IT asset minimum and maximum sparing levels.
b. IT asset thresholds for executing sparing replenishment.
c. Available IT asset spare quantities.
d. IT assets spares consumed and replenished during the quarter.
e. Abnormal IT asset failure trends.
f. Failure analysis for abnormal IT asset failures.

C.5.4.3.2.3 COST PROJECTIONS

The contractor shall deliver an **O&M Cost Projection Estimate** (Section F, Deliverable 42) that identifies all the projected costs for O&M tools (e.g., service contracts, licenses renewals, and life cycle replacements) and ODCs for the next Government FY, identified per month and per quarter.

C.5.4.3.3 CHANGE MANAGEMENT AND RELEASE MANAGEMENT

The contractor shall centrally manage and control the implementation of all changes to the infrastructure services and devices including corrective patches and service packs, and required upgrades. The contractor shall manage all changes in accordance with DHS Infrastructure Change Control Board (ICCB) and St. Elizabeths Information Technology Change Control Board (SEITCCB) processes and policies. The contractor shall implement approved requests in accordance with contractor-defined Release Management processes.

The contractor shall report implementation status, for approved change requests, to the SEITCCB prior to the Board meeting, until the request is fully implemented or withdrawn. The contractor shall capture changes within the St. Elizabeths Campus IT infrastructure change management services. Changes may include, but are not limited to:

a. Completing, for all new installations, system upgrades, changes, additions, or routine maintenance, all requested administrative requirements and testing prior to submission to Government Governance approval.
b. Assessment of Government-directed security patches or service packs before implementation to verify the need to implement and the impact upon the system.
c. In coordination with the Government, determination of the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs.
d. Providing monthly reports to the appropriate Government-designated representative on the success of the patch/service pack deployment and any issues preventing completion.

The contractor shall provide change requests to the St. Elizabeths Campus Governance Boards. Change requests shall identify requested changes to IT infrastructure or to configuration items. Unique change requests shall be tracked and updated weekly using Government services until the change request is closed by the Government.

The contractor shall provide a **Change and Release Management Report** (Section F, Deliverable 43), that identifies the CIs (e.g., hardware, software, drawings, and connections) that have been updated or changed since the last Government-accepted Change and Release Management Report and shall also identify quarterly and year-to-date statistics and trend analysis for CIs that are driving IT Service Desk incidents.

C.5.4.3.4 CONFIGURATION MANAGEMENT

The contractor shall manage and maintain baseline configurations for St. Elizabeths Campus IT infrastructure. The contractor shall ensure that baseline changes are controlled in a Government services CMDB in accordance with industry and Government best practices (e.g., ITIL).

The contractor shall ensure that the CMDB and the CIs (e.g., software, software licenses and installation keys, software scripts, IP addresses, physical configurations, and system configurations) are accessible to the IT Service Desk services to allow for CMDB and CI call up for incidents, requests, and work orders.

The contractor shall prepare an **O&M Configuration Management Plan (CMP)** (Section F, Deliverable 44) that describes the contractor's approach, management and processes for change management, release management, and CI management of St. Elizabeths Campus IT infrastructure. The CONOPS defines the St. Elizabeths Campus Governance Boards and authority.

C.5.4.3.5 ROUTINE AND MECHANICAL MAINTENANCE

The contractor shall conduct routine and mechanical maintenance for the St. Elizabeths Campus IT infrastructure. The St. Elizabeths Campus IT infrastructure consists of IT assets that will require routine maintenance (e.g., cleaning and calibration) and mechanical maintenance (e.g., turnstiles, x-ray machines, and access control systems). Some IT assets requiring maintenance are elevated requiring special assistance (e.g., ladders, mechanical lifts, and rooftop access) or special equipment and tools.

The contractor shall prepare a **Maintenance Plan** (Section F, Deliverable 46) that describes devices requiring maintenance, the steps for performing said maintenance, and the frequency of said maintenance.

C.5.4.3.5.1 UNINTERRUPTIBLE POWER SUPPLY (UPS) MAINTENANCE

The contractor shall perform preventative maintenance on Uninterruptible Power Supplies (UPS). Preventative maintenance comprises of visual inspections (e.g., connections, burned insulation, liquid contamination, and damage), cleaning, connection tightening, and routine testing (e.g., monitored battery-rundown test).

C.5.4.3.6 BACKUP AND RECOVERY

The contractor shall develop a St. Elizabeths Campus **IT Infrastructure Backup and Recovery Plan** (Section F, Deliverable 47). The St. Elizabeths Campus IT Infrastructure Backup and Recovery Plan shall identify the St. Elizabeths Campus infrastructure hardware and software configurations and applications settings and the processes and procedures for executing backup and recovery to include required testing and periodicity. The contractor shall identify and ensure critical software applications and the associated hardware and licenses are available to enable re-installation on replacement equipment and re-imaging of existing devices.

The contractor shall conduct routine testing in accordance with the St. Elizabeths Campus IT Infrastructure Backup and Recovery Plan.

C.5.4.3.7 KNOWLEDGE MANAGEMENT

The contractor shall maintain a Knowledge Management Service that is a comprehensive repository of standard operational processes and procedures in accordance industry and Government best practices. This includes lessons learned, engineering documentation, drawings, external vendor documentation, and other O&M information. The Knowledge Management Service shall be available to the IT Service Desk and other authorized personnel.

The contractor shall prepare a **Knowledge Management Index** (Section F, Deliverable 48) that indexes and categories the Knowledge Management Services. The Knowledge Management Index shall identify active, updated, and achieved knowledge.

C.5.4.3.8 ACCOUNT ADMINISTRATION

The contractor shall perform account administration for the St. Elizabeths Campus IT infrastructure. Account administration includes the creation, on Government authorization, activation, maintenance, suspension, and deactivation of access, user, system, and administrative accounts.

The contractor shall deactivate or suspend access, user, system, and administrative accounts in accordance with DHS 4300B.102 National Security Systems Security Control Guidance unless the account is otherwise waived or superseded of this requirement by the Government.

The contractor shall prepare an **Account Administration Report** (Section F, Deliverable 49) that identifies all access, user, system, and administrative accounts correlated to the St.

Elizabeths IT infrastructure. The Account Administration Report shall identify all accounts activated and deactivated or suspended since the last Government-accepted Account Administration Report and any accounts that have been inactive for more than 30, 60, or 90 calendar days.

C.5.4.4 SUBTASK 4 – IT SECURITY MANAGEMENT

The contractor shall perform IT Security Management to ensure the CIA of the St. Elizabeths Campus IT infrastructure, and provide IT Security reports required by DHS IT Security Policy or DHS OCIO.

The contractor shall prepare an **IT Security Status Report** (Section F, Deliverable 50) that describes IT security work completed, work planned for the next reporting period, and issues and concerns.

The contractor shall prepare a **Security Controls Review Report** (Section F, Deliverable 51) that identifies any new Government direction effecting corresponding security controls and validating the security controls that were updated in response to Government direction since the last Government-accepted Security Controls Review Report.

C.5.4.4.1 IT SECURITY COMPLIANCE

The contractor shall ensure St. Elizabeths Campus IT infrastructure is in compliance with Government IA requirements.

The contractor shall support the security processes, controls, and tools that provide IA for the St. Elizabeths Campus IT infrastructure in accordance with DHS 4300A Sensitive Systems Handbook, DHS 4300B National Security Systems Policy Directive, DHS Management Directives (MDs), the NIST SP 800 Series, Risk Management Framework (NIST SP 800-37), Director of Central Intelligence Directives (DCID), and the Intelligence Community Directives (ICD).

The contractor shall directly support the Government (e.g., DHS Risk Management Division (RMD)) in the oversight of security compliance (i.e., FISMA) of all IT infrastructure issues relative to Government security policies, directives, and regulations.

The contractor shall perform the following in support of Government security compliance programs:

a. C&A:
    i. Support the development and review of IT infrastructure security documentation
b. Information Systems Security Officer (ISSO):
    i. Maintain IA accreditations (e.g., ATO).
    ii. Maintain operational and situational awareness through the continued monitoring of the IT infrastructure and conduct reviews of IT infrastructure security scans.
    iii. Identify and report IT infrastructure security event, notifications, and deficiencies to the Government (e.g., Information Systems Security Manager (ISSM) and ISSO)
    iv. Provide IT infrastructure security support to the SOC.
    v. Provide IT infrastructure security vulnerability management support to the SOC.

c. Evaluate and validate that all changes to the IT infrastructure comply with Government security controls, processes, and procedures.
d. Deploy and maintain guards and gateways (e.g., firewalls and IDS) to monitor, prevent, detect, respond, report, and correct the unauthorized release of unclassified and classified data.

The contractor shall develop a St. Elizabeths Campus **IT Security Management Plan** (Section F, Deliverable 52). The St. Elizabeths Campus IT Security Management Plan shall identify and describe how the contractor shall comply with DHS 4300A Sensitive Systems Handbook and DHS 4300B National Security Systems Policy Directive**.**

C.5.4.4.2 IT SECURITY LOGS, RETENTION, AND REVIEW

Access to St. Elizabeths Campus IT infrastructure security logs shall be restricted to ISSM-designated and approved contractor personnel, Government personnel, and other Government contractors.

The contractor shall maintain all IT security logs including:

a. Managing in accordance with retention period requirements.
b. Recording all accesses to security logs, including an audit history of reads, changes, and deletions.
c. Protecting logs under these restrictions to include all security logs (e.g., PEP, IDS, anti-virus) as well as domain controller and all management systems as directed by the ISSM and ISSO.
d. Performing reviews and providing responses and data to ad hoc inquiries and data requests on all IT security system logs.

C.5.4.4.3 IT SECURITY EVENTS AND INCIDENT RESPONSE

The contractor shall provide IT security events and incident response services and capabilities to respond to St. Elizabeths Campus IT infrastructure events and incidents that impact the CIA and the IA posture of the IT infrastructure in accordance with DHS 4300A Sensitive Systems Handbook Attachment F Incident Response.

Per DHS 4300A Sensitive Systems Handbook Attachment F Incident Response, the St. Elizabeths Campus operates as a “Component Security Operations Center” and shall be subject to all “Component Security Operations Center” event and incident response requirements.

“Events” and “Incidents” are defined per DHS 4300A Sensitive Systems Handbook Attachment F Incident Response Section 2.2 Definitions.

The contractor shall report events and incidents per DHS 4300A Sensitive Systems Handbook Attachment F Incident Response Section 3.7 Incident Reporting Process Flow and DHS 4300A Sensitive Systems Handbook Attachment F Incident Response Appendix F5 **DHS Security Incident Report Form** (Section F, Deliverable 53).

The contractor shall report events and incidents to the St. Elizabeths Campus ISSMs and ISSOs.

The contractor shall develop a St. Elizabeths Campus **IT Incident Response Plan** (Section F, Deliverable 54). The St. Elizabeths Campus IT Incident Response Plan shall identify and describe how the contractor shall comply with DHS 4300A Sensitive Systems Handbook Attachment F Incident Response.

C.5.4.5 SUBTASK 5 – TECHNICAL MANAGEMENT

The contractor shall provide O&M technical management services under this Subtask. Technical management provides oversight of all O&M technical services ensuring personnel, processes, and procedures are available and technically capable of delivering O&M services to meet performance standards. Technical management facilitates the management of suppliers, vendors, manufacturers, and events and utilizes information and data to identify opportunities for improvement and increased efficiencies. Technical management additionally monitors workload and identifies and obtains specialized resources as required to resolve incidents, requests, and work orders. Technical management coordinates educational briefings about the St. Elizabeths Campus IT infrastructure as requested by the Government.

The contractor shall coordinate technical management with Task 2 - Requirements Analysis and Design and Task 3 - Implement, Test, and Secure Services to ensure full system engineering life cycle considerations.

The contractor shall develop and maintain an **IT Service Management Architectural Framework** (Section F, Deliverable 55) that describes and identifies the CIs and depository locations for CIs. At a minimum, the IT Service Management Architectural Framework shall include:

a. IT infrastructure ISP (e.g. building layouts, blueprints, wiring diagrams, floor plan layouts, cabling layout, and rack elevations).

b. IT infrastructure OSP (e.g., conduit runs, manholes, pull holes, and butterfly drawings).

c. IT infrastructure facilities (e.g., power/grounding, primary and backup power, fire suppression, and monitoring devices).

d. IT infrastructure active equipment configurations (e.g., IP Addresses, VLAN, firewalls, routers, switches, servers, virtualized hardware, and storage devices).

e. IT infrastructure software (e.g., database software, operating systems, system utilities, software inventory, and virtualization software).

f. Files and databases (e.g., data architecture, data dictionaries, and database schemas).

g. Operating infrastructure (asset management system, auto discovery system, backup/restore tools, change management system, configuration management software, and definitive media library).

h. IT infrastructure maintenance Standard Operating Procedures (SOPs) (e.g., routine maintenance, backups, optimizations, and storage defragmentation).

i. IT Infrastructure Preventative Maintenance SOPs (e.g., cleaning, mechanical, and inspections).

j. Processes (e.g., SOPs, incidents, requests, work orders, and security incident response).

k. Vendors, suppliers, and manufacturers' information (e.g., contact list, service contracts, and sales representatives).

C.5.4.5.1 SERVICE LEVEL MANAGEMENT (SLM)

The contractor shall perform SLM to meet the St. Elizabeths Campus IT infrastructure SLAs. The CONOPS defines the specific St. Elizabeths Campus IT infrastructure SLA metrics and calculations. The contractor shall ensure that incidents, requests, and work orders are accurately categorized, associated, and status reported with the appropriate SLAs.

The contractor shall be responsible for identifying any incidents, requests, or work orders to the Government that the contractor deems should be excluded from the SLAs.

The contractor shall evaluate SLA metrics and as required recommend changes, additions, or deletions to the Government where the recommendation improves or enhances the performance monitoring accuracy and coverage of the IT infrastructure.

C.5.4.5.2 OPERATIONAL PLANNING

The contractor shall work with the Government to identify requests and work orders that require the development of cost estimates and schedules.

The contractor shall prepare and maintain a St. Elizabeths Campus IT Infrastructure **Service Description Document** (Section F, Deliverable 78). At a minimum, the Service Description Document shall include for each service: title, status (e.g., planned, deployed, or terminated), classification/physical infrastructure (e.g., SBUCAN, SCAN, or TSCAN), short description (e.g., general), long description (e.g., technical), capabilities (e.g., primary or optional), prerequisites (e.g., software), and configurations. The Service Description Catalog shall directly or via reference identify associated CIs, SLAs, service support agreements, service assets, and suppliers.

The contractor shall prepare and maintain an **IT Service Catalog** (Section F, Deliverable 56) that describes standard work order requests (e.g., adding security camera) with associated cost estimates for labor and materials to complete standard work order requests.

C.5.4.5.3 EDUCATIONAL PRESENTATIONS

The contractor shall prepare and deliver educational presentations to contractor personnel, Government personnel, and other Government contractors on the St. Elizabeths Campus IT infrastructure and O&M operations.

Historically these presentations have occurred monthly to senior Government personnel.

C.5.4.5.4 O&M SERVICE IMPROVEMENTS

The contractor shall monitor and review operational and performance data as well as technical execution of policies, procedures, and processes to identify and improve operational performance. At a minimum, the contractor shall:

a. Review IT Service Desk incidents, requests, and work orders and determine and identify opportunities for automating recurring incidents, requests, and work orders (e.g., password resets).
b. Identify IT assets with a recurring failure rate, instability, or reliability issues.
c. Identify policies, procedures, and processes or concerns that are negatively impacting customer satisfaction, or performance.

d. Identify and resolve instances of non-compliance with policies, procedures, and processes.

The contractor shall identify and describe recommended performance improvements (e.g., policies, procedures, and processes) to the Government in the MSR or other appropriate deliverable. The description shall include an issues statement, analysis of alternatives, and the recommended solution(s).

C.5.5 TASK 5 - IT INFRASTRUCTURE TRANSITIONAL SERVICES

The contractor shall provide IT infrastructure transitional services to DHS Component Agencies relocating the St. Elizabeths Campus. IT infrastructure transitional services include the evaluation, preparation, and integration of each DHS Component Agency's IT infrastructure into the St. Elizabeths Campus IT infrastructure. IT infrastructure transitional services also include the temporary extension of the St. Elizabeths Campus IT infrastructure to each DHS Component Agency's legacy facility prior to DHS Component Agency relocations to the St. Elizabeths Campus.

The contractor shall use a systems engineering methodology in evaluating and preparing each DHS Component Agency's IT infrastructure for operations and integration into the St. Elizabeths Campus IT infrastructure. The preparation of each DHS Component Agency's IT infrastructure shall meet or exceed the Government's approved requirements and ensure that the DHS Component Agency's IT infrastructure is technically feasible, proficient, integrated and interoperable, and in compliance with Government architectures, standards, design guides, and policies.

The contractor's IT infrastructure transitional services for each DHS Component Agency's IT infrastructure equipment, technology, and solutions shall be Government approved by the following:

a. The HLSEA TRM Standards and Products Profiles (Section H.3, GFI).

b. Where applicable be on the DHS Enterprise Architecture Information Repository.

c. Where applicable be certified under the NIAP Common Criteria.

d. Where applicable be certified under the FIPS.

e. Where applicable be certified by the JITC.

f. Where applicable be on the DoD UC APL.

g. Where applicable be on the FICAM PACS APL.

When the contractor recommends or when DHS Component Agency's IT infrastructure equipment, technology, or solutions that are not Government approved or do not comply with Government, organization, or industry standards and protocols, the contractor shall:

a. Comply with all policies and procedures for the introduction of new equipment, technology, and solutions per:

    i. C&A.

    ii. ATO.

    iii. HLSEA TRM.

  iv. DHS Enterprise Architecture Information Repository.

b. Coordinate with DHS MGMT/OCIO/ITSO/EDMO through the ITSO/CRMD/St. Elizabeths Special Program Office.
c. Coordinate with the DHS and St. Elizabeths Campus IT infrastructure Governance Boards.

The contractor shall utilize and improve upon industry and Government best practices, processes, and procedures for delivering IT infrastructure transitional services.

Based on the Enhanced Plan, it is anticipated that IT infrastructure transitional services will take place during Option Period One, Option Period Two, and Option Period Three of the TO.

Anticipated Transitional Services, based on future DHS vision:

a. 75 percent of seats relocated to the St. Elizabeths Campus will receive St. Elizabeths Campus VoIP services prior to relocation.

Anticipated Transitional Services, based on projected historical trends:

a. One conference room upgraded (e.g., A/V and VTC) and customized (e.g., Senior Executive) per 1,000 seats relocated to the St. Elizabeths Campus.
b. One server or application upgraded and migrated to DHS DC-1 and DC-2 per 500 seats relocated to the St. Elizabeths Campus.

C.5.5.1 SUBTASK 1 - TRANSITIONAL SERVICES MANAGEMENT

The contractor shall comply and execute transitional services management in accordance with the DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, the DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, and other industry and Government systems engineering best practices (e.g., PMBOK, ITIL, and PRINCE2).

The Government will assign “project” status to IT infrastructure transitional services activities for DHS Component Agencies relocating to the St. Elizabeths Campus. The Government will organize projects into an overarching St. Elizabeths Campus IT infrastructure portfolio.

The contractor shall support transitional services management of the St. Elizabeths Campus IT infrastructure project portfolio by performing the following services:

a. Develop and manage to project plans.
b. Develop and manage to project WBSs.
c. Develop and manage to project schedules.
d. Develop and manage to costs.
e. Identify and manage to risks and issues.
f. Identify, coordinate, and manage IT infrastructure transitional services activities with contractor personnel, Government personnel, and other Government contractors.
g. Identify and report any deviations, substitutions, or other modifications to Government-approved designs to the Government.
h. Identify, coordinate, and manage communications (e.g., technical, schedules, and risks) with contractor personnel, Government personnel, and other Government contractors.

i. Identify, coordinate, and manage the reporting of project status with contractor personnel, Government personnel, and other Government contractors.

j. Identify, coordinate, and manage implementation, testing, and securing activities with contractor personnel, Government personnel, and other Government contractors.

k. Identify, coordinate, and manage the reporting of testing status with contractor personnel, Government personnel, and other Government contractors.

l. Identify, coordinate, and manage the transitioning of IT infrastructure to O&M services.

m. Identify, coordinate, and manage the transfer of artifacts and CIs (e.g., drawings and licenses) to O&M services.

The contractor shall develop a St. Elizabeths Campus **IT Infrastructure Transitional Services Master Plan** (Section F, Deliverable 57). The St. Elizabeths Campus IT Infrastructure Transitional Services Master Plan shall identify and describe how the contractor shall comply with DHS Guidebook 102-01-103-01 Systems Engineering Life Cycle Guidebook, DHS Directives System Instruction Number: 102-01-103 System Engineering Life Cycle, DHS 4300A Sensitive Systems Handbook, DHS 4300B National Security Systems Policy Directive, and other industry and Government systems engineering best practices.

C.5.5.2 SUBTASK 2 - EVALUATION OF IT INFRASTRUCTURE

The contractor shall coordinate and communicate with each DHS Component Agency’s contractor personnel, Government personnel, and other Government contractors to identify DHS Component Agency IT infrastructure that will be relocating to the St. Elizabeths Campus, and St. Elizabeths IT infrastructure that will be temporarily extended to each DHS Component Agency’s legacy facility.

The contractor shall conduct DHS Component Agency IT infrastructure surveys to collect and document DHS Component Agency IT infrastructure.

The contractor shall develop a **DHS Component Agency IT Infrastructure Transitional Services Report** (Section F, Deliverable 58) for each DHS Component Agency relocating to the St. Elizabeths Campus. The DHS Component Agency IT Infrastructure Transitional Services Report shall include, as a minimum, the following:

a. List of DHS Component Agency’s POCs (i.e., name, title, e-mail, and telephone).

b. List of DHS Component Agency’s IT infrastructure that will require integration into the St. Elizabeths Campus IT infrastructure.

c. List of DHS Component Agency’s IT infrastructure that will require connectivity to the St. Elizabeths Campus IT infrastructure.

d. List of DHS Component Agency’s IT infrastructure that will be discontinued (e.g., sunset), terminated, or will otherwise not be available via the St. Elizabeths Campus IT infrastructure.

e. Identify St. Elizabeths Campus IT infrastructure (e.g., VoIP) that will be temporarily extended to DHS Component Agency’s legacy facilities.

f. Identify changes that require submission and approval of Government Change Control Boards (e.g., ICCB, SEITCCB).

g. Identify DHS Component Agency's IT infrastructure special or unique requirements (e.g., technical and performance).
h. Identify DHS Component Agency's IT infrastructure that is non-interoperable or would otherwise degrade the St. Elizabeths Campus IT infrastructure's Confidentiality, Integrity, or Availability (CIA).
i. Identify DHS Component Agency's IT infrastructure technical actions to be completed prior to relocation of the DHS Component Agency to the St. Elizabeths Campus.
j. Identify any risks (e.g., technical, performance, and schedule).

C.5.5.3 SUBTASK 3 - PREPARATION OF IT INFRASTRUCTURE

The contractor shall coordinate and communicate with each DHS Component Agency's contractor personnel, Government personnel, and other Government contractors to prepare (e.g., configure, upgrade, engineer, or discontinue) DHS Component Agency infrastructure for relocation to the St. Elizabeths Campus and for temporarily extending St. Elizabeths Campus IT infrastructure to each DHS Component Agency's legacy facility.

The contractor shall develop a **DHS Component Agency IT Infrastructure Transitional Services Plan** (Section F, Deliverable 59) for each DHS Component Agency relocating to the St. Elizabeths Campus. The DHS Component Agency IT Infrastructure Transitional Services Plan shall include the following:

a. Configuration:
    i. Identify DHS Component Agency's IT infrastructure that requires configuration (e.g., firewalls).
    ii. Document DHS Component Agency's IT infrastructure's updated configuration settings.
    iii. Identify St. Elizabeths Campus IT infrastructure that requires configuration (e.g., routers).
    iv. Document St. Elizabeths Campus IT infrastructure's new configuration settings.
    v. Identify responsibility for each reconfiguration.
    vi. Identify responsibility for Government Change Control Board submissions.
b. Upgrading:
    i. Identify DHS Component Agency's IT infrastructure that requires upgrades (e.g., hardware products and software versions).
    ii. Identify St. Elizabeths Campus IT infrastructure standards or baselines.
    iii. Identify responsibility for each upgrade.
    iv. Identify responsibility for Government Change Control Board submissions.
c. Engineering:
    i. Identify DHS Component Agency's IT infrastructure that requires engineering changes for interoperability with St. Elizabeths Campus IT infrastructure.
    ii. Document (i.e., EIP) DHS Component Agency's IT infrastructure's engineering changes.

iii. Identify St. Elizabeths Campus IT infrastructure that requires engineering changes for interoperability with DHS Component Agency's IT infrastructure.

iv. Document (i.e., EIP) St. Elizabeths Campus IT infrastructure's engineering changes (e.g., new dedicated PTP connectivity and new VLAN).

v. Identify responsibility for each engineering change.

vi. Identify responsibility for Government Change Control Board submissions.

d. Schedule of configuration, upgrading, and engineering activities.

C.5.5.4 SUBTASK 4 - INTEGRATION OF IT INFRASTRUCTURE

The contractor shall coordinate and communicate with each DHS Component Agency's contractor personnel, Government personnel, and other Government contractors to execute configuration, upgrading, engineering, and discontinuation of each DHS Component Agency's IT infrastructure for relocation to the St. Elizabeths Campus.
The contractor shall execute in accordance with the Government-approved DHS Component Agency IT Infrastructure Transitional Services Plan.

C.5.5.5 SUBTASK 5 - TRANSITION AND TRANSFER TO O&M

The contractor shall develop a **DHS Component Agency IT Infrastructure Transition and Transfer to O&M Checklist** (Section F, Deliverable 60) for each DHS Component Agency relocating to the St. Elizabeth's Campus, which identifies all the DHS Component Agency's IT infrastructure to be transitioned to Task 4 O&M Services. The DHS Component Agency IT Infrastructure Transition and Transfer to O&M Checklist shall list all artifacts and CIs that are to be transferred to Task 4 O&M Services upon completion of Task 5 IT Infrastructure Transitional Services projects. The DHS Component Agency IT Infrastructure Transition and Transfer to O&M Checklist shall identify the transition and transfer dates for DHS Component Agency IT infrastructure, artifacts, and CIs.

The contractor (e.g., O&M Lead) shall review, verify, and sign each DHS Component Agency's IT Infrastructure Transition and Transfer to O&M Checklist. The contractor shall obtain Government signature on DHS Component Agency IT Infrastructure Transition and Transfer to O&M Checklists. On Government signature, the Task 5 IT Infrastructure Transitional Services project is complete.

C.5.5.6 SUBTASK 6 - DISASSEMBLE, STAGE, AND REASSEMBLE IT ASSETS

The contractor shall coordinate, manage, and perform the disassembly and staging of DHS Component Agency IT assets at DHS Component Agency legacy facilities prior to relocating to the St. Elizabeths Campus.

The contractor will not be responsible for the physical movement of IT assets from DHS Component Agency legacy facilities to the St. Elizabeths Campus.

The contractor shall coordinate, manage, and perform the staging and assembly of DHS Component Agency IT assets on the St. Elizabeths Campus.

C.5.6 TASK 6 - TASK ORDER TRANSITION SUPPORT SERVICES

The contractor shall provide transition-in and transition-out support services under the TO and ensure uninterrupted services with no degradation in capabilities.

C.5.6.1 SUBTASK 1 – PROVIDE TRANSITION-IN SUPPORT

The contractor shall ensure a smooth and orderly transition-in to establish required support. The contractor shall update the Draft Transition-In Plan provided with its proposal and provide a **Final Transition-In Plan** (Section F, Deliverable 63). The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition-in. The contractor shall implement its transition-in approach at TOA. The contractor shall complete all transition-in activities and achieve full operational O&M capability (e.g., steady state) during the TO's base period.

The transition-in activities shall implement the contractor's DHS Supply Chain Risk Management (SCRM) approach.

C.5.6.1.1 CONTRACTOR IT SECURITY PLAN AND ACCREDITATION

The contractor shall provide, implement, and maintain a Contractor IT Security Plan. The Contractor IT Security Plan shall describe the processes and procedures that will be followed to ensure appropriate IT security training of contractor personnel and the security of Government and contractor IT resources that are developed, processed, or used under this TO to include the secure communications of Government information (e.g., For Official Use Only (FOUO)). The Contractor IT Security Plan shall identify essential requirements (e.g., critical incident response) and corresponding list of supporting personnel (i.e., essential personnel) to include personnel contact information to the Government. The list shall contain the individual's name, address, home phone number, mobile phone number, work phone number, security clearance, and duty title. The Government will treat the provide list as Personal Identifiable Information (PII).

The contractor shall deliver a **Contractor IT Security Plan** (Section F, Deliverable 64) on which the Government will make comments. The contractor shall incorporate the Government-approved Contractor IT Security Plan, into the TO as a compliance document.

The Contractor IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; the FISMA of 2002; and with Federal policies and procedures include the OMB Circular A-130. The Contractor IT Security Plan shall specifically include instructions regarding handling and protecting sensitive information at the contractor's site (including any information stored, processed, or transmitted using the contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

After TOA, the contractor shall submit written proof of **Contractor IT Security Accreditation** (Section F, Deliverable 66) to the Government (i.e., DHS OCIO Risk Management Division (RMD)) for approval. Accreditation shall proceed according to the criteria of the DHS Sensitive System Policy Publication 4300A version 12. This accreditation shall include the final IT Security Plan. This accreditation, when accepted by the Government, shall be incorporated into the TO as a compliance document. The contractor shall comply with the approved accreditation documentation.

C.5.6.1.2 BASELINE OF PHYSICAL IT INFRASTRUCTURE

The contractor shall conduct a review, survey, and audit of the St. Elizabeths Campus physical IT infrastructure and prepare a **Baseline Configuration Utilization Report** (Section F, Deliverable 67). The Configuration Utilization Report shall identify and document the physical IT infrastructure (e.g., OSP conduit, OSP fiber, server rack space, patch panels, power panels), the utilization of the physical IT infrastructure, and as applicable, the source and destination connections and other applicable information. During the survey and audit, the contractor shall ensure all physical IT infrastructure is appropriately labeled and tagged.

The contractor shall update the Government services CMDB and CIs, based on the Baseline Configuration Utilization Report, 30 calendar days after Government approval. The updated Government services CMDB and CIs establish the baseline for the St. Elizabeths Campus physical IT infrastructure.

C.5.6.1.3 TRANSFER OF MATERIALS AND TOOLS

The contractor shall coordinate and transfer materials and tools from warehouse facilities located at Railroad Avenue, SE, Washington, D.C. 20020.

The contractor shall process, inventory, and reconcile materials and tools in Government Asset Management Services and in accordance with Task 4 (C.5.4.3.2 Asset Management).

The contractor shall prepare and deliver a **Transferred Materials and Tools Report** (Section F, Deliverable 68). The Transferred Materials and Tools Report shall identify and document all materials and tools transferred and any discrepancies and reconciliations.

C.5.6.2 SUBTASK 2 – PROVIDE TRANSITION-OUT SUPPORT

The contractor shall facilitate and conduct transition-out support under the TO. Transition-Out shall ensure no disruption to vital Government business. The contractor shall provide full cooperation to provide necessary operational knowledge transfer to the incoming contractor(s). The contractor shall provide all documentation to Government personnel.

The contractor shall perform the following during Transition-Out:

a. Implement project management processes.
b. Identify POCs.
c. Identify location of technical and project management documentation.
d. Provide status of ongoing technical initiatives.
e. Implement contractor-to-contractor coordination with Government oversight to ensure a seamless transition.
f. Transition Key Personnel functions and information.
g. Identify schedules and milestones.
h. Identify actions required of the Government.
i. Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

The contractor shall provide a **Transition-Out Plan** (Section F, Deliverable 69) for transitioning and delivering all material, tools, and information from the TO to the Government. The Transition-Out Plan shall identify all Government-Furnished and Contractor-Furnished Material (GFM/CFM) as well as information and material developed during the TO that was used in the execution of this TO.

On final Government acceptance of the contractor's Transition-Out Plan, the contractor shall follow the Transition-Out Plan to transfer all material, information, and rights thereto to the Government.

The contractor shall prepare a **Transition-Out Technical Report** (Section F, Deliverable 71) documenting the status of all ongoing efforts and projects (e.g., building IT design), including copies of all plans, policies, procedures, POCs, and other information required by the Government.